(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 721 275**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/62 (2013.01)
G06Q 20/20 (2012.01)
G06Q 20/34 (2012.01)
G06F 21/31 (2013.01)
G06F 21/85 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.06.2016 E 16177228 (0)**

(97) Fecha y número de publicación de la concesión europea: **23.01.2019 EP 3113056**

(54) Título: **Protección de una validación de una secuencia de caracteres, procedimiento, dispositivo y programa informático correspondientes**

(30) Prioridad:

03.07.2015 FR 1556352

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.07.2019

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

GERAUD, RÉMI;
KOUDOUSSI, HIBA y
NACCACHE, DAVID

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Protección de una validación de una secuencia de caracteres, procedimiento, dispositivo y programa informático correspondientes

1. Sector

El sector de la invención es el de los dispositivos electrónicos de obtención de datos utilizados para realizar operaciones que hacen intervenir o utilizan objetos de naturaleza confidencial. A título ilustrativo, se pueden citar operaciones de pago que hacen intervenir un número de tarjeta bancaria o que utilizan una entrada de código confidencial asociado a una tarjeta de pago. Otras operaciones tales como, por ejemplo, operaciones de tipo médico o civil, que utilizan datos biológicos o patrimoniales de un individuo, están relacionados asimismo con la presente técnica.

2. Técnica anterior

Ciertos dispositivos electrónicos de introducción de datos, tales como los terminales de pago, por ejemplo, están diseñados específicamente, tanto en hardware como en software, para ofrecer la protección más óptima posible de los datos confidenciales susceptibles de ser introducidos. Esta protección contra intrusiones o ataques se puede realizar en varios niveles. Al nivel de la constitución física del dispositivo electrónico de introducción de datos, su estructura puede consistir, por ejemplo, en una carcasa inviolable, resistente a una manipulación indebida («tamper resistant», en inglés), o que deja un rastro visible de cualquier intento de sabotaje («tamper evident», en inglés), o incluso que proporciona una respuesta adaptada a una detección de manipulación indebida («tamper responsive», en inglés). La utilización de circuitos electrónicos grabados en la masa o multicapa puede proporcionar asimismo una protección mejorada del dispositivo, lo que hace mucho más compleja la tarea de personas malintencionadas que buscan interceptar datos confidenciales por medio de sensores colocados en ciertas conexiones del dispositivo. Al nivel de la constitución funcional del dispositivo, los datos sensibles están, en general, cifrados y su procesamiento está sujeto a protocolos criptográficos. Finalmente, a nivel de software, en general, es preferible utilizar componentes aptos para ser implementados únicamente dentro de procesadores seguros que son inaccesibles a terceros.

Un inconveniente de este importante nivel de protección es que la flexibilidad de utilización ofrecida por tales dispositivos sigue siendo limitada. La certificación de una aplicación para que pueda ser autorizada su ejecución en el procesador seguro del dispositivo a menudo es larga y obligatoria. En un mundo rico en equipos electrónicos diversos, tales como teléfonos móviles, asistentes personales o microordenadores, existe la necesidad de una flexibilidad comparable para los dispositivos de introducción de datos que se utilizan para realizar operaciones que hacen intervenir o utilizan objetos de carácter confidencial, llamados asimismo dispositivos seguros. Se sabe que los sistemas operativos comúnmente denominados abiertos ofrecen una gran cantidad de aplicaciones útiles y fáciles de utilizar que es interesante poder implementar para satisfacer esta necesidad de flexibilidad en los dispositivos seguros. Asimismo, cada vez más dispositivos electrónicos seguros de introducción de datos comprenden, además del procesador seguro, un procesador no seguro capaz de ejecutar aplicaciones de terceros, por ejemplo, telecargables en una plataforma de distribución puesta a disposición por el fabricante del dispositivo. El documento EP1788507 describe, por ejemplo, un dispositivo seguro del tipo de terminal de pago, que comprende dos entornos de ejecución, un entorno de ejecución seguro para la ejecución de las aplicaciones seguras y un entorno de ejecución no seguro para la ejecución de las aplicaciones no seguras, disponiendo cada entorno de su propio procesador. Esta apertura de otras aplicaciones de software distintas de las rigurosamente protegidas tiene el inconveniente de poner potencialmente en peligro la seguridad de los datos introducidos en el dispositivo seguro. De este modo, una aplicación maliciosa (o contaminada por secuencias de ejecución maliciosas), podría espiar y traicionar procesos de protección del equipo, para recuperar información confidencial. Una aplicación maliciosa podría imitar asimismo la apariencia de una aplicación legítima (por ejemplo, una aplicación de pago) para engañar a un usuario y, de este modo, recuperar su información confidencial.

A medida que el gran público comienza a estar sensibilizado frente a la existencia de estas técnicas fraudulentas en los terminales de comunicaciones personales (tabletas, teléfonos inteligentes, microordenadores, etc.), no tiene necesariamente el mismo nivel de vigilancia frente a dispositivos más especializados (tales como los terminales de pago) que, no obstante, forman parte integrante de su vida cotidiana, pero que supone que son seguros por la naturaleza de las operaciones que son procesadas rutinariamente. Por lo tanto, tiende a darles su confianza de manera más natural, a pesar de que el riesgo de que le roben datos confidenciales sigue estando presente.

Por consiguiente, existe la necesidad de proponer dispositivos electrónicos de introducción de datos que comprendan medios para evitar o ralentizar los intentos de recuperar datos confidenciales de manera fraudulenta.

3. Resumen

La invención propone un procedimiento de protección, un dispositivo electrónico de introducción de datos y un programa informático telecargable tales como los definidos en las reivindicaciones.

La técnica propuesta ofrece una solución que no presenta al menos algunos de estos problemas de la técnica anterior, gracias a un procedimiento original para proteger la validación de una secuencia de caracteres introducida por un usuario en un dispositivo electrónico de introducción de datos que comprende un procesador no seguro y un procesador seguro. Según un primer aspecto de la técnica propuesta, este procedimiento es puesto en práctica en el procesador seguro, y comprende una etapa para determinar el procesamiento que se aplicará a la secuencia de caracteres introducida, en función de una señal representativa de una validación, por parte del usuario, de esta secuencia de caracteres. La señal representativa de una validación es entregada por un medio de validación que pertenece a un conjunto que comprende al menos dos medios de validación separados, disponibles en el dispositivo electrónico de introducción de datos.

De este modo, la técnica propuesta permite diferenciar, al nivel de un procesador seguro de un dispositivo electrónico de introducción de datos, el procesamiento que se aplicará a una secuencia de caracteres introducidos por un usuario en este dispositivo, en función de un medio de validación de dicho dispositivo utilizado por el usuario para validar esta secuencia de caracteres introducida. De esta manera, es especialmente posible asignar más particularmente un primer medio de validación (dicho medio de validación segura) de dicho dispositivo a la validación de información considerada como sensible (la validación de un código confidencial asociado a una tarjeta de pago, por ejemplo), y un segundo medio de validación (dicho medio de validación no segura), diferente del primero, a la validación de la información considerada poco o nada sensible (la validación de una cantidad a pagar, por ejemplo).

En un modo de realización particular de la técnica propuesta, la etapa de determinación de un procesamiento a aplicar a la secuencia de caracteres comprende:

- una etapa de obtención de la señal representativa de una validación de dicha secuencia de caracteres,

- una etapa de obtención, en una memoria segura, de dicha secuencia de caracteres;

- cuando la señal es representativa de una validación no segura:

  - una etapa de transmisión de dicha secuencia de caracteres a una aplicación común;

  - una etapa de supresión, de dicha memoria segura, de dicha secuencia de caracteres.

De esta manera, una secuencia de caracteres cuya introducción es validada por el medio de validación no segura es sistemáticamente transmitida a la aplicación común en curso de ejecución en el dispositivo electrónico de introducción de datos, sin ninguna otra forma de verificación. La aplicación común corresponde, en general, a la aplicación que se está ejecutando en el dispositivo electrónico de introducción de datos, y cuya interfaz gráfica se muestra en la pantalla de dicho dispositivo en el momento de la validación de la secuencia de caracteres introducida previamente. Puede ser ejecutada por el procesador seguro o por el procesador no seguro y, la mayoría de las veces, es la aplicación en el origen de la solicitud de introducción de información, formulada al usuario (por ejemplo, por medio de un mensaje, mostrado en una pantalla del dispositivo, y que invita al usuario a introducir una información de una naturaleza determinada), que condujo a la introducción y validación de dicha secuencia de caracteres.

En un modo de realización particular de la técnica propuesta la etapa de determinación de un procesamiento a aplicar a la secuencia de caracteres comprende, además, cuando la señal es representativa de una validación segura:

- una etapa de comparación de la aplicación común con una lista predeterminada de aplicaciones;

  - cuando dicha aplicación común está presente en la lista predeterminada de aplicaciones:

    - una etapa de transmisión de dicha secuencia de caracteres a dicha aplicación común;

    - una etapa de supresión, de dicha memoria segura, de dicha secuencia de caracteres;

- cuando dicha aplicación común está ausente de la lista de aplicaciones predeterminada, una etapa de supresión, de dicha memoria segura, de dicha secuencia de caracteres.

De esta manera, cuando se utiliza el medio de validación segura para validar la introducción de una secuencia de caracteres, el procesador seguro realiza una verificación adicional para determinar el procesamiento a aplicar a esta secuencia de caracteres. Si parece que la aplicación común no pertenece a una lista predeterminada de aplicaciones - en otras palabras, si no parece legítimo que la aplicación común requiera el empleo de una validación segura para la información que se introduce - la secuencia de caracteres introducida por el usuario es pura y simplemente descartada (es decir, eliminada de la memoria segura asociada al procesador seguro). Por consiguiente, no es transmitida a la aplicación común (ya sea porque esta aplicación es sospechosa, o porque el usuario ha utilizado inadvertidamente el medio de validación segura para validar su introducción, en lugar del medio de validación no segura que habría debido ser empleado con respecto a la naturaleza de la aplicación común), y los datos introducidos, potencialmente confidenciales, no están comprometidos. A la inversa, si parece legítimo emplear el medio de validación segura con respecto a la aplicación común (esta última forma parte, en realidad, de la lista

predeterminada de aplicaciones), entonces la secuencia de caracteres introducida es transmitida a esta aplicación común.

En otro modo de realización particular de la técnica propuesta, el procedimiento de protección comprende, además, cuando la aplicación común está ausente de la lista predeterminada de aplicaciones, una etapa de visualización, en una pantalla del dispositivo electrónico de introducción de datos, de un dato representativo de la supresión sin transmisión de dicha secuencia de caracteres.

De esta manera, el usuario puede ser advertido, por ejemplo, por medio de un mensaje mostrado en la pantalla del dispositivo electrónico de introducción de datos, que la secuencia de caracteres ha sido suprimida sin ser transmitida a la aplicación común, y se le explican las razones.

En otro modo realización particular más de la técnica propuesta, la longitud de la secuencia de caracteres obtenida en la memoria segura está predefinida.

De este modo, la longitud de la secuencia de caracteres almacenada en la memoria segura asociada al procesador seguro puede ser adaptada en función de las características de los datos confidenciales que pueden ser introducidos en el tipo de dispositivo considerado. Por ejemplo, en un terminal de pago, una información confidencial que comúnmente se introduce es el código de identificación personal (código PIN) de cuatro dígitos asociado a una tarjeta de pago. Limitando, por lo tanto, la longitud de la secuencia de caracteres almacenada en la memoria segura a los últimos cuatro caracteres introducidos, se garantiza la protección de un posible código de identificación personal introducido, sin bloquear completamente la aplicación común en su funcionamiento común cuando no se lleve a cabo una validación (siendo transmitidos a la aplicación común los caracteres que no forman parte de las últimas cuatro entradas, cuando el usuario introduce nuevos caracteres). Esta limitación del número de caracteres almacenados en la memoria segura permite asimismo protegerse contra potenciales ataques en el procesador seguro: de este modo, una persona maliciosa no podrá, por ejemplo, comprometer el procesador seguro, introduciendo una gran cantidad de caracteres sin realizar nunca la validación.

En otro modo de realización particular de la técnica propuesta, la secuencia de caracteres es suprimida de la memoria segura del dispositivo de introducción de datos electrónicos si no se realiza una nueva introducción de caracteres en el dispositivo durante un tiempo predeterminado.

De este modo, el tiempo de guardado de datos potencialmente confidenciales en el dispositivo electrónico de introducción de datos es limitado: sin acción por parte del usuario después de transcurrido un tiempo determinado, estos datos son suprimidos particularmente de la memoria segura asociada al procesador seguro. Esto constituye una medida de protección adicional, ya que los datos introducidos por un usuario en el dispositivo electrónico de introducción de datos, incluso si no son validados, solo se guardan temporalmente en este dispositivo.

En un modo de realización particular de la técnica propuesta, El dispositivo electrónico de introducción de datos es un terminal de pago.

Según otro aspecto, la técnica propuesta se refiere asimismo a un dispositivo electrónico de introducción de datos que comprende un procesador no seguro y un procesador seguro, y que comprende medios de protección de una validación de una secuencia de caracteres introducida por un usuario. Un dispositivo electrónico de introducción de datos de este tipo comprende:

- un conjunto que comprende al menos dos medios de validación separados;

- medios de determinación, por parte de dicho procesador seguro, de un procesamiento a aplicar a dicha secuencia de caracteres, en función de una señal representativa de un medio de validación, utilizada por dicho usuario para validar dicha secuencia de caracteres, siendo enviada dicha señal representativa de una validación por uno de los medios de validación pertenecientes a dicho conjunto que comprende al menos dos medios de validación separados.

Según una implementación preferida, las distintas etapas del procedimiento de protección según la técnica propuesta son puestas en práctica mediante uno o varios programas o programas informáticos, que comprenden instrucciones de software destinadas a ser ejecutadas por un procesador de datos según la técnica propuesta y están diseñados para controlar la ejecución de las diversas etapas de los procedimientos.

En consecuencia, la técnica propuesta se dirige también a un programa, susceptible de ser ejecutado por un ordenador o por un procesador de datos, y, en particular, a un procesador seguro, comprendiendo este programa instrucciones para controlar la ejecución de las etapas de un procedimiento tal como el mencionado anteriormente en el presente documento.

Este programa puede utilizar cualquier lenguaje de programación, y estar en forma de código fuente, código objeto o de código intermedio entre el código fuente y el código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

La técnica propuesta también se dirige a un soporte de información legible por un procesador de datos, y que comprende instrucciones de un programa tal como el mencionado anteriormente en el presente documento.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una ROM, por ejemplo, un CD ROM o una ROM de circuitos microelectrónicos, o incluso un medio de grabación magnética, por ejemplo, un disquete (disco flexible) o un disco duro.

Por otra parte, el soporte de información puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede ser encaminada a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la técnica propuesta puede ser telecargado, en particular, en una red de tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que está incorporado el programa, estando adaptado el circuito para ejecutar el procedimiento en cuestión o para ser utilizado en la ejecución del mismo.

Según un modo de realización, la técnica propuesta es puesta en práctica por medio de componentes de software y/o hardware. Con esto en mente, el término «módulo» puede corresponder igualmente en este documento a un componente de software, que a un componente de hardware corresponde o a un conjunto de componentes de software o de hardware.

Un componente de software corresponde a uno o a varios programas informáticos, a una o a varias subrutinas de un programa, o, de manera más general, a cualquier elemento de un programa o de un software capaz de poner en práctica una función o un conjunto de funciones, tal como se describe a continuación en el presente documento para el módulo en cuestión. Un componente de software de este tipo es ejecutado por un procesador de datos de una entidad física (terminal, servidor, puerta de enlace, encaminador, etc.) y puede acceder a los recursos de hardware de esta entidad física (memorias, soportes de grabación, bus de comunicación, tarjetas electrónicas de entradas / salidas, interfaces de usuario, etc.).

De la misma manera, un componente de hardware corresponde a cualquier elemento de un conjunto físico (o hardware) capaz de poner en práctica una función o un conjunto de funciones, según lo que se describe a continuación para el módulo en cuestión. Se puede tratar de un componente de hardware programable o un procesador integrado para la ejecución de software, por ejemplo, un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un firmware (firmware), etc.

Por supuesto, cada componente del sistema descrito anteriormente pone en práctica sus propios módulos de software.

Las diferentes realizaciones mencionadas anteriormente en el presente documento pueden ser combinadas entre sí para la puesta en práctica de la invención.

4. Lista de las figuras

Otras características y ventajas de la invención aparecerán más claramente con la lectura de la siguiente descripción de un modo de realización preferente de la invención, dada a título de simple ejemplo ilustrativo y no limitativo, y de los dibujos adjuntos, entre los cuales:

- la figura 1 describe un ejemplo de dispositivo electrónico de introducción de datos, tal como el que existe en la técnica anterior;

- la figura 2 presenta un dispositivo electrónico de introducción de datos, en el que la introducción de información se realiza por medio de pulsadores físicos, en un modo de realización particular de la técnica propuesta;

- la figura 3 presenta un dispositivo electrónico de introducción de datos, en el que la introducción de información se realiza mediante pulsadores virtuales mostrados en una pantalla táctil, en un modo de realización particular de la técnica propuesta;

- la figura 4 describe una arquitectura simplificada de un entorno de ejecución seguro que comprende un procesador seguro, en el que se puede poner en práctica el procedimiento de protección de una validación de una secuencia de caracteres, según un modo de realización particular de la técnica propuesta;

- la figura 5 ilustra las etapas puestas en práctica al nivel de un procesador seguro de un dispositivo electrónico de introducción de datos, para llevar a cabo el procedimiento de protección de una validación de una secuencia de caracteres, según un modo de realización particular de la técnica propuesta;

- la figura 6 presenta un ejemplo de secuencia de caracteres almacenada en una memoria segura asociada al procesador seguro, cuando un usuario realiza entradas en el teclado de un dispositivo electrónico de introducción de datos, según un modo de realización particular de la técnica propuesta.

5. Descripción detallada

5.1 Contexto general

La técnica propuesta se aplica más particularmente a los dispositivos electrónicos de introducción de datos que comprenden dos procesadores, un procesador seguro y un procesador no seguro. El procesador seguro tiene acceso a una memoria segura, y la asociación de estos dos elementos forma, por consiguiente, un entorno de ejecución seguro en el dispositivo. Para un entorno de ejecución seguro, se entiende una protección que puede ser tanto de hardware como de software, en particular con la puesta en práctica de las diferentes técnicas de protección presentadas en relación con la técnica anterior (constitución física de la carcasa de protección de los componentes seguros, circuitos electrónicos grabados en la masa o multicapa, cifrado de los datos, etc.). Esta protección se basa asimismo en la utilización, al nivel del procesador seguro, de un sistema operativo seguro, en el sentido de que dispone de un conjunto de medios (de control, de restricción de acceso, criptográficos, etc.) orientado a hacerlo menos vulnerable y a protegerlo de manera eficaz de cara a los diferentes tipos de ataques que podría sufrir. A la inversa, el sistema operativo puesto en práctica en el procesador no seguro del dispositivo electrónico de introducción de datos es un sistema que se puede calificar de «sistema abierto» en el sentido de que el acceso suficiente a este sistema está ampliamente disponible, lo que favorece el desarrollo de numerosas aplicaciones. El concepto de sistema operativo abierto, por consiguiente, engloba no solo a los sistemas operativos realmente abiertos, tales como los sistemas UNIX y LINUX originales, sino también a los sistemas de gran difusión comercial tales como son, por ejemplo, las diferentes versiones de Microsoft Windows™. El interés de tales dispositivos - que comprenden tanto un procesador seguro como un procesador no seguro - reside en su capacidad de poder poner en práctica no solo aplicaciones seguras, en el sentido de que, con mucha frecuencia, han sido certificadas por un organismo de confianza y están autorizadas para ser ejecutadas por el procesador seguro, pero también por aplicaciones de terceros, no necesariamente certificadas. Estas aplicaciones de terceros, ejecutadas por el procesador no seguro, permiten enriquecer la experiencia del usuario y permiten abrir el dispositivo a nuevas funcionalidades. En relación con la figura 1, se presenta un dispositivo electrónico de introducción de datos (10) de este tipo, tal como el que existe en la técnica anterior. Un dispositivo (10) de este tipo comprende con mucha frecuencia una pantalla (11), que permite mostrar la interfaz gráfica de una aplicación común ejecutada en el dispositivo, y un teclado (12), que permite a un usuario interactuar con dicha aplicación. El teclado (12) comprende tradicionalmente varios conjuntos de teclas. Un primer conjunto, denominado en el presente documento conjunto de las teclas de entrada (13), agrupa las teclas que permiten al usuario introducir información en el dispositivo. Estas teclas están asociadas, en general, a uno o varios caracteres alfanuméricos o de puntuación. Mediante pulsaciones sucesivas sobre estas teclas de entrada, un usuario tiene, de este modo, la posibilidad de formar una secuencia de caracteres, representativa, por ejemplo, del monto de una transacción financiera o de un código confidencial asociado a una tarjeta de pago. Un segundo conjunto de teclas, denominado en el presente documento conjunto de las teclas de control (14), agrupa las teclas que permiten a un usuario actuar sobre una secuencia de caracteres introducida previamente por medio de las teclas de entrada (13). Están dispuestas teclas para validar (V), corregir (C) o anular (X) una secuencia de caracteres introducida previamente. Otras teclas, que no son ni teclas de entrada ni teclas de control y que están agrupadas en el presente documento bajo el término genérico de conjunto de teclas auxiliares (15), pueden finalmente completar el teclado (12). Se puede tratar, por ejemplo, de teclas de navegación, de función, de acceso directo, etc.

En un dispositivo electrónico de introducción de datos (10) de este tipo, las aplicaciones seguras son puestas en práctica por un procesador seguro (PS), mientras que las aplicaciones de terceros, no seguras, son puestas en práctica por un procesador no seguro (PNS). El procesador no seguro (PNS) está dispuesto, en general, bajo el control del procesador seguro (PS), en una relación del tipo principal - secundario. En particular, cualquier dato proveniente del procesador no seguro o destinado al mismo pasa a través del procesador seguro. En este contexto, el procesador seguro es particularmente capaz de interceptar cualquier dato introducido por un usuario en el teclado (12) de dicho dispositivo, incluso si la introducción de estos datos ha sido solicitada por una tercera aplicación ejecutada por el procesador no seguro (PNS). Por otra parte, cuando se utiliza un dispositivo electrónico de introducción de datos (10) de este tipo para la realización de una transacción segura que implica la introducción de datos confidenciales (por ejemplo, una operación de pago), los medios de interacción del dispositivo con un usuario (tales como la pantalla (11), el teclado (12), un lector de tarjeta, etc.) pasa de manera integral a estar bajo el control del procesador seguro (PS). El procesador no seguro (PNS) ya no puede interactuar con estos elementos, lo que garantiza una protección reforzada de estas operaciones sensibles, ya que solo las aplicaciones certificadas ejecutadas al nivel del procesador seguro tienen entonces la posibilidad de acceder a los datos intercambiados.

El dispositivo presentado en relación con la figura 1, que comprende un teclado físico, se ofrece a título puramente ilustrativo y no limitativo. En particular, las consideraciones anteriores relacionadas con los diferentes conjuntos de teclas presentes en un teclado siguen siendo aplicables, por supuesto, en el caso de un teclado virtual mostrado en una pantalla táctil de dicho dispositivo. Sucede, asimismo, que el dispositivo electrónico de introducción de datos no comprende más que un procesador principal, capaz de realizar sucesivamente la función de procesador seguro por una parte y de procesador no seguro por otra parte. En este caso, el entorno de ejecución seguro toma la forma de un modo específico de ejecución de este procesador principal del dispositivo electrónico de introducción de datos.

En el resto del documento, se considera, a efectos de simplificación, que el dispositivo electrónico de introducción de datos es un terminal de pago electrónico. Este ejemplo se ofrece a título puramente ilustrativo y no limitativo, y la

técnica propuesta puede ser puesta en práctica en otros tipos de dispositivos electrónicos de introducción de datos, tales como teléfonos inteligentes o tabletas, sin apartarse del alcance de la presente técnica.

En la mayoría de los dispositivos electrónicos de introducción de datos existentes, una sola y única tecla de validación única está dedicada, en general, a la validación de cualquier operación que requiera la confirmación de una entrada realizada previamente por un usuario. El teclado de un terminal de pago, tal como el que se presenta, por ejemplo, en la figura 1, comprende de este modo convencionalmente una sola tecla de validación (la mayoría de las veces asociada al color verde) destinada a confirmar cualquier entrada de un usuario (en el ejemplo presentado, se trata de la tecla (V), comprendida en el conjunto de teclas de control (14)). Cualquiera que sea la naturaleza de la operación en curso en el dispositivo electrónico de introducción de datos, esta misma tecla de validación se utiliza para confirmar cualquier secuencia de caracteres introducida por el usuario. De este modo, por ejemplo, la tecla de validación (V) puede ser utilizada en un primer momento por un comerciante para validar la cantidad a pagar por un cliente a continuación de una operación de compra, habiendo sido introducida esta cantidad previamente por medio de las teclas de entrada (13). A continuación, el comerciante presenta el terminal de pago (10) al cliente, quien verifica la cantidad mostrada en la pantalla (11), introduce el código confidencial asociado a su tarjeta de pago previamente introducida en el dispositivo, y a su vez utiliza la misma tecla de validación (V) para confirmar la introducción correcta de su código confidencial y, de este modo, activar la operación de pago.

Con estos dispositivos electrónicos de introducción de datos existentes, que no ofrecen más que un medio de validar una secuencia de caracteres introducida por un usuario, la misma tecla de validación se utiliza tanto para validar una operación inocua (por «inocua», se entiende una operación no crítica, que no hace intervenir datos sensibles, la introducción de una cantidad, por ejemplo), como una operación crítica (que utiliza datos sensibles, la introducción de un código confidencial, por ejemplo). Por otra parte, también se puede observar que, con los dispositivos existentes, esta misma tecla de validación ha sido utilizada asimismo tanto para validar una operación solicitada por una aplicación de terceros no segura (ejecutada por un procesador no seguro) como para validar una operación solicitada por una aplicación segura (ejecutada por el procesador seguro).

El inconveniente de este planteamiento es que ofrece a personas malintencionadas la oportunidad de burlar la vigilancia de los usuarios de dichos dispositivos electrónicos de introducción de datos. Siendo los mecanismos de validación actualmente similares, tanto al nivel de la naturaleza de las operaciones (inocua frente a crítica) como de su origen (solicitadas por una aplicación no segura frente a solicitada por una aplicación segura), las técnicas de suplantación de identidad (o «phishing» en Inglés) - que consisten en robar los datos confidenciales de un usuario por medio de una aplicación maliciosa que imita a una aplicación legítima - por lo tanto, pueden revelarse particularmente eficaces.

La técnica descrita en el presente documento se propone remediar, al menos en parte, este problema, por una parte, por medio de un dispositivo electrónico de introducción de datos que comprende al menos dos medios separados de validación de una secuencia de caracteres introducida, y, por otra parte, mediante la puesta en práctica de un proceso de protección de la validación de dicha secuencia de caracteres introducida, procedimiento que tiene en cuenta el medio utilizado para validar dicha introducción.

5.2 Dispositivo

En relación con la figura 2, se presenta un ejemplo de un dispositivo electrónico de introducción de datos en un modo de realización particular de la invención. Tal como ya se describió en la presentación general del contexto general de la invención, este dispositivo comprende dos procesadores (no representados): un procesador seguro para la puesta en práctica de aplicaciones seguras, y un procesador no seguro para la puesta en práctica de aplicaciones de terceros no seguras. A diferencia de un dispositivo electrónico de introducción de datos convencional, tal como el que ya se presentó en relación con la figura 1, el dispositivo descrito en el presente documento comprende un conjunto que comprende al menos dos medios de validación distintos que se pueden utilizar para validar una secuencia de caracteres previamente introducida: un medio de validación denominado seguro (VS) y un medio de validación llamado no seguro (VNS). En el ejemplo de la figura 2, estos medios de validación son pulsadores físicos. Con el fin de no molestar a los usuarios acostumbrados a utilizar un dispositivo electrónico de introducción de datos convencional, el pulsador de validación segura (VS) está dispuesto de manera ideal en el mismo sitio que ocupa tradicionalmente el único pulsador de validación de un dispositivo equivalente de la técnica anterior (ocupa la misma posición, en la cara delantera, abajo a la derecha en el ejemplo de las figuras 1 y 2: el medio de validación segura (VS) de la figura 2 está posicionado en el sitio del medio de validación convencional (V) de la figura 1). Este medio de validación segura (VS) está dispuesto bajo el control exclusivo del procesador seguro, por ejemplo, gracias a un cableado físico exclusivo. En un modo de realización particular del dispositivo propuesto, el pulsador de validación no segura (VNS) está aislado del resto del teclado, de tal manera que esté relativamente alejado del pulsador de validación segura (VS). El pulsador de validación no segura (VNS) está posicionado, por ejemplo, en una cara del dispositivo, que es diferente de la que acoge al resto del teclado. Si el resto del teclado está integrado, como es, en general el caso, en la cara delantera del dispositivo electrónico de introducción de datos, el pulsador de validación no segura (VNS) está posicionado, por ejemplo, en el borde del dispositivo lo más alejado posible del pulsador de validación segura, o incluso en la cara posterior. De esta manera, el acceso a este pulsador de validación no segura se hace más difícil, y su posición y su utilización se presentan como inusuales para un usuario (por ejemplo, un cliente).

En el caso en el que lo esencial del teclado del dispositivo electrónico de introducción de datos no está constituido por un teclado físico, sino por un teclado virtual mostrado en una pantalla táctil, se aplica igualmente el mismo principio general que consiste en ofrecer dos medios separados de validación - una validación segura, dispuesta bajo el control del procesador seguro y una validación no segura. En relación con la figura 3, se presenta otro modo de realización particular de un dispositivo de este tipo, que comprende una pantalla táctil (31) capaz de mostrar, entre otros elementos gráficos, un teclado virtual. Esta pantalla táctil (31) está dividida en al menos dos zonas: una zona denominada no segura (32) y una zona denominada segura (33). La zona no segura (32) define una parte de la pantalla táctil dentro de la cual cualquier aplicación - ya sea ejecutada por el procesador seguro o por el procesador no seguro - puede mostrar datos y recopilar señales de presiones en un lugar de dicha zona. Por lo que respecta a la zona segura (33) está dispuesta bajo el control exclusivo del procesador seguro: solo una aplicación segura ejecutada por el procesador seguro está en condiciones de mostrar y de recopilar información. Es en esta zona en la que se muestra el medio de validación segura (VS), que se encuentra asimismo bajo el control exclusivo del procesador seguro. También se pueden mostrar en esta zona segura otros pulsadores táctiles de control (no representados), tales como un pulsador de corrección o un pulsador de anulación de la entrada, en la que el procesador no seguro no tiene ningún control: no tiene acceso a esta zona, ya sea para mostrar en ella elementos o para interceptar eventos (pulsaciones realizadas por un usuario) que se producirían en la misma. El medio de validación no segura (VNS) se muestra, por su parte, en el área no segura (32) de la pantalla táctil, eventualmente bajo el control de una aplicación no segura.

Las dos realizaciones particulares del dispositivo electrónico de introducción de datos presentadas en las figuras 2 y 3 se facilitan a título puramente ilustrativo y no limitativo. Otras combinaciones son posibles, siempre y cuando el medio de validación segura (VS) permanezca colocado bajo el control exclusivo del procesador seguro.

Además del conjunto que comprende al menos los dos medios de validación separados que son los medios de validación segura (VS) y no segura (VNS), el dispositivo electrónico de introducción de datos comprende asimismo medios de determinación de un procesamiento a aplicar a la secuencia de caracteres introducidos, en función de una señal representativa del medio de validación utilizado por el usuario para validar dicha secuencia de caracteres. Esta señal representativa de una validación es emitida por uno de los medios de validación que pertenecen al conjunto que comprende al menos dos medios de validación separados. En otras palabras, es emitida después de una pulsación, por parte del usuario, sobre uno de los pulsadores (táctiles o físicos) que constituyen los medios de validación segura (VS) y no segura (VNS).

Estos medios de determinación de un procesamiento a aplicar son puestos en práctica por un procesador seguro, al nivel de un entorno de ejecución seguro tal como el presentado en relación con la figura 4.

Por ejemplo, el entorno de ejecución seguro incluye una memoria segura (41) constituida por una memoria temporal, una unidad de procesamiento (42), equipada, por ejemplo, con el procesador seguro, y controlada por el programa informático seguro (43), que pone en práctica las etapas necesarias para la protección de una validación de una secuencia de caracteres según la técnica propuesta.

Al inicio, las instrucciones de código del programa informático (43) son cargadas, por ejemplo, en una memoria, antes de ser ejecutadas por el procesador seguro de la unidad de procesamiento (42). La unidad de procesamiento (42) recibe en la entrada (E), por ejemplo, una señal representativa de una validación, después de la utilización por parte del usuario del dispositivo electrónico de introducción de datos, de uno de los medios de validación que pertenecen al conjunto que comprende al menos dos medios de validación separados. El procesador seguro de la unidad de procesamiento (42) pone en práctica, a continuación, las etapas de un procedimiento de protección de la validación de la secuencia de caracteres previamente introducida por el usuario, según las instrucciones del programa informático (43), y determina en la salida (S) el procesamiento a aplicar a dicha secuencia de caracteres, en función de la señal representativa de una validación.

Para ello, el entorno de ejecución seguro comprende, además de la memoria segura (41), medios de transmisión / recepción de datos, que permiten, por una parte, el intercambio de datos provenientes de un dispositivo de entrada (por ejemplo, un teclado) y con destino a un dispositivo de restitución (por ejemplo, una pantalla) del dispositivo electrónico de introducción de datos, y por otra parte el intercambio de datos con un procesador no seguro del dispositivo electrónico de introducción de datos. De este modo, el entorno de ejecución seguro es particularmente capaz de interceptar los datos provenientes de una aplicación ejecutada en el procesador no seguro del dispositivo electrónico de introducción de datos o con destino a la misma. Estos medios de transmisión / recepción de datos pueden materializarse en forma de interfaces de conexión de software o interfaces de hardware. Según la técnica propuesta, un entorno de ejecución seguro de este tipo comprende, además, medios de almacenamiento que pueden tomar la forma de una base de datos o de un conjunto de archivos de configuración, o un acceso a medios de almacenamiento de este tipo. Estos medios de almacenamiento pueden, en particular, alojar una lista predeterminada de aplicaciones, que enumera las aplicaciones en las que la utilización de un medio de validación segura se considera legítima. Entre estas aplicaciones, se pueden citar a modo de ejemplo las aplicaciones seguras o certificadas, ejecutadas, en general, por el procesador seguro, que hacen intervenir o requieren la introducción de datos confidenciales, por ejemplo, una aplicación de pago. No obstante, esta lista no está limitada a este tipo de aplicaciones, y puede comprender asimismo aplicaciones ejecutadas por el procesador no seguro, pero que, por ejemplo, son bien conocidas y ampliamente utilizadas (tales como las aplicaciones de caja), y para las cuales

imponer la utilización del medio de validación no seguro, por su posición inusual, parecería contraproducente o demasiado molesto para un usuario. Esta lista de aplicaciones es actualizada, por ejemplo, por el fabricante del dispositivo electrónico de introducción de datos.

5.3 Procedimiento

A continuación, se describen, en relación con la figura 5, las etapas puestas en práctica al nivel del procesador seguro de un dispositivo electrónico de introducción de datos, para la realización del procedimiento de protección de una validación de una secuencia de caracteres, según un modo de realización particular de la técnica propuesta. El dispositivo electrónico de introducción de datos comprende al menos dos medios para validar una secuencia de caracteres introducida, tal como se expuso anteriormente: un medio de validación segura (VS) colocado bajo el control exclusivo del procesador seguro, y un medio de validación no segura. En el modo de realización particular presentado en relación con la figura 5, una aplicación común (AppC), segura o no, se está ejecutando, y transmite información con destino a un usuario por medio, por ejemplo, de una interfaz gráfica mostrada en la pantalla del dispositivo electrónico de introducción de datos. La aplicación común (AppC) puede invitar especialmente al usuario a introducir información con el objetivo de continuar una transacción.

Durante una etapa de interceptación 51, el procesador seguro intercepta las entradas realizadas por un usuario en el teclado (físico o táctil) del dispositivo electrónico de introducción de datos, hasta la obtención de una señal (SIG_V) representativa de una validación de dicha introducción. De este modo, a cada pulsación del usuario sobre una tecla de introducción de dicho teclado y siempre que no se obtenga una señal representativa de una validación, el carácter asociado es interceptado y almacenado en una memoria segura asociada al procesador seguro. El conjunto de los caracteres introducidos forma a continuación una secuencia de caracteres (SEQ) grabada en la memoria segura asociada al procesador seguro. En el modo de realización propuesto en relación con la figura 5, la interceptación de los caracteres introducidos y el almacenamiento, en dicha memoria, de la secuencia de caracteres (SEQ) resultante, se mantienen mientras que no se obtenga la señal de validación (SIG_V). Esta señal de validación (SIG_V) se obtiene cuando el usuario ha terminado la introducción de una secuencia de caracteres deseada y la valida utilizando uno de los dos medios de validación (no segura o segura) puestos a su disposición en el dispositivo electrónico de introducción de datos. Según el medio utilizado por el usuario para validar su secuencia de caracteres, la señal obtenida es representativa de una validación no segura o de una validación segura (esta información se obtiene, por ejemplo, determinando qué tecla de validación física ha sido pulsada o, en el caso de un teclado táctil, detectando las coordenadas de la zona de pulsación y deduciendo la naturaleza del pulsador de validación táctil asociado).

Una vez recibida la señal (SIG_V), el procesador seguro recupera, en la memoria segura asociada, la secuencia de caracteres (SEQ), durante una etapa para obtención 52 de dicha secuencia de caracteres.

Cuando la señal obtenida durante la etapa de interceptación 51 es representativa de una validación no segura, se transmite la secuencia de caracteres (SEQ) obtenida durante la etapa de obtención 52, (etapa de transmisión 53), a la aplicación común (AppC) en el origen de esta solicitud de introducción de información. En particular, puede tratarse de una aplicación de terceros ejecutada en el procesador no seguro. En este caso, no existe ningún control, por así decirlo, por parte del procesador seguro, de la legitimidad que tiene o no la aplicación común para solicitar información a un usuario. Se considera que el usuario sabe lo que hace, en la medida en la que utiliza especialmente un medio de validación particular - el pulsador de validación no segura – preferentemente situado en una posición de acceso menos fácil que el resto del teclado (en el caso contrario, en el que una aplicación malintencionada se haría pasar por una aplicación legítima e insistiría para que un usuario confiado valide datos confidenciales por medio de este pulsador de validación no segura, la posición particular e inusual de este último tiene por efecto, de manera ideal, despertar las sospechas de este usuario).

Cuando se realiza esta transmisión, la secuencia de caracteres (SEQ) puede para ser suprimida (etapa de supresión 54) de la memoria segura asociada al procesador seguro.

Cuando la señal obtenida en el curso de la etapa de interceptación 51 es representativa de una validación segura, el procesador seguro pone en práctica una etapa de comparación (55) de la aplicación común (AppC) con una lista predeterminada de aplicaciones, para determinar el procesamiento a aplicar a la secuencia de caracteres (SEQ) obtenida (en el curso de la etapa de obtención 52). La aplicación común considerada es la que está activa al momento de pulsar el pulsador de validación segura (es decir, por ejemplo, la aplicación a la que está asociada la interfaz gráfica mostrada en la pantalla del dispositivo electrónico de introducción de datos, en el momento de la validación.) La comparación de la aplicación común con la lista predeterminada de aplicaciones se puede realizar en función de diferentes criterios, por ejemplo, un nombre o un identificador de la aplicación. También puede ser puesta en práctica sobre la base de marcadores informáticos (o indicadores, «flag», en inglés) específicos y seguros, que solo el procesador seguro puede implementar para «marcar» ciertas aplicaciones particulares, en particular las aplicaciones que hacen intervenir datos sensibles. La propia ausencia de tales marcadores define asimismo una naturaleza de la aplicación común: en este caso de figura, se tiene que tratar normalmente con una aplicación en relación con datos de naturaleza no crítica, para los cuales la utilización de una validación segura normalmente no tiene sentido. Por lo que respecta a la lista predeterminada de aplicaciones, identifica las aplicaciones en las cuales la utilización de un medio de validación segura se considera legítimo (son, en general, pero no necesariamente

siempre es el caso, aplicaciones para las cuales parece legítimo que el procesamiento de los datos relacionados permanezca en el perímetro exclusivo del procesador seguro). Se trata, particularmente, de aplicaciones que hacen intervenir datos confidenciales, tales como transacciones de pago que implican la introducción de datos bancarios, de un código confidencial asociado a una tarjeta de pago o de crédito, información sensible de naturaleza médica o civil, que está relacionada con datos biológicos o patrimoniales específicos para una persona, etc.

En el caso de que esté presente la aplicación común (AppC) en la lista predeterminada de aplicaciones, la secuencia de caracteres (SEQ) obtenida es transmitida, durante una etapa de transmisión 56, a la aplicación común (AppC) en el origen de esta solicitud de introducción de información. Este caso de figura corresponde al caso nominal en el que parece legítimo que el usuario se sirva del pulsador de validación segura para confirmar una entrada previamente realizada, con respecto a la aplicación común que se está ejecutando. La secuencia de caracteres (SEQ) introducida forma a continuación, en cualquier caso, un dato confidencial o sensible, por lo que es deseable que sea gestionado exclusivamente al nivel del procesador seguro del dispositivo electrónico de introducción de datos. Una vez que se ha llevado a cabo esta transmisión de la secuencia de caracteres (SEQ) a la aplicación común (AppC), la secuencia de caracteres (SEQ) puede ser suprimida de la memoria segura asociada al procesador seguro (etapa de supresión 57).

En el caso contrario, en el que la aplicación común (AppC) está ausente de la lista predeterminada de aplicaciones, la secuencia de caracteres (SEQ) es suprimida de la memoria segura asociada al procesador seguro (etapa de supresión 58). Por lo tanto, no se transmite a la aplicación común (AppC). De hecho, el procesador seguro detecta entonces una validación segura en asociación con una aplicación común que, en cualquier caso, no debería requerir una validación de este tipo. Este caso de figura puede corresponder a un error de manipulación por parte del usuario (que ha utilizado el pulsador de validación segura en lugar de utilizar el pulsador de validación no segura), o a un intento de fraude: por consiguiente, conviene no transmitir la secuencia de caracteres (SEQ) introducida a la aplicación común (AppC) y, pura y simplemente, es suprimida. En un modo de realización particular de la técnica propuesta, un dato representativo de la supresión sin transmisión de dicha secuencia de caracteres (por ejemplo, un mensaje de advertencia) se puede mostrar, a continuación, en la pantalla del dispositivo electrónico de introducción de datos, a fin de advertir al usuario que su entrada no ha sido procesada, explicando los motivos.

En un modo de realización particular de la técnica propuesta, la lista predeterminada de aplicaciones contiene únicamente aplicaciones susceptibles de ser ejecutadas por el procesador seguro del dispositivo electrónico de introducción de datos. De esta manera, siempre que la señal obtenida sea representativa de una validación segura, la secuencia de caracteres (SEQ) nunca se transmite al procesador no seguro y permanece exclusivamente en el seno del procesador seguro.

El procedimiento descrito anteriormente es puesto en práctica al nivel del procesador seguro del dispositivo electrónico de introducción de datos, por ejemplo, por medio de una aplicación o de un proceso seguro exclusivo (diferente de la aplicación común (AppC)) ejecutado en este procesador seguro, estando dicha aplicación o proceso seguro constantemente «a la escucha», en segundo plano. Desde que se detecta la validación de una primera secuencia de caracteres previamente introducida, el procedimiento puede ser completado y conducir, según el caso, a la transmisión o a la supresión de dicha primera secuencia de caracteres. A continuación, es puesto en práctica de nuevo inmediatamente, a fin de proteger la validación de la siguiente secuencia de caracteres introducida.

En un modo de realización particular de la técnica propuesta, el procesador seguro envía a la aplicación común (AppC) una señal representativa de una pulsación sobre una tecla de entrada, cada vez que el usuario introduce un carácter por medio de una tecla de entrada del dispositivo electrónico de introducción de datos. Esta señal no contiene ninguna información de una naturaleza que permita la identificación del carácter introducido. De este modo, esta señal permite notificar a la aplicación común (AppC) que se ha introducido un carácter, sin que, sin embargo, le permita identificar este carácter. De esta manera, la aplicación común (AppC) es capaz de mostrar una retroalimentación visual al usuario a medida que escribe, antes de que se realice una validación. La aplicación común puede, por ejemplo, hacer mostrar un asterisco en una pantalla del dispositivo electrónico de introducción de datos, cada vez que un usuario introduce un carácter. Se informa a este usuario en tiempo real que se tiene en cuenta su introducción. Este mecanismo permite asimismo a la aplicación común (AppC) compatibilizar el número de caracteres ya introducidos por un usuario, a fin de verificar que se alcance una cantidad de caracteres esperados, por ejemplo.

En otro modo de realización particular de la técnica propuesta, la secuencia de caracteres actual grabada, a medida que el usuario la escribe, en la memoria segura asociada al procesador seguro, es suprimida de dicha memoria si el usuario no realiza ninguna introducción de carácter o ninguna validación en el dispositivo electrónico de introducción de datos durante un tiempo predeterminado. En otras palabras, si el procesador seguro no detecta ni una nueva introducción de carácter, ni validación durante un tiempo predeterminado (por ejemplo, unos diez segundos o un minuto), suprime la secuencia de caracteres actualmente en espera en la memoria segura.

Según aún otro modo de realización particular de la técnica propuesta, el número de caracteres de la secuencia de caracteres que el procesador seguro puede conservar en la memoria segura es limitado y predeterminado. Por lo tanto, imponer una longitud máxima predefinida a la secuencia de caracteres que se guarda en la memoria segura tiene varias ventajas. En primer lugar, esto permite que la aplicación común (AppC) obtenga, bajo ciertas

condiciones, una retroalimentación después de las introducciones de caracteres realizadas por un usuario, sin tener que esperar necesariamente una acción de validación de la secuencia de caracteres introducida, y esto sin sacrificar, por lo tanto, la protección de eventuales datos confidenciales introducidos. Por ejemplo, si se considera un terminal de pago cuya funcionalidad principal es permitir la realización de operaciones de pago por medio de tarjetas de pago convencionales, que están asociadas a códigos confidenciales de cuatro dígitos, la longitud máxima de la secuencia de caracteres memorizada en el marco del procedimiento propuesto puede ser fijada en cuatro caracteres (puesto que proteger los cuatro últimos caracteres introducidos antes de una validación es, por lo tanto, a priori, suficiente para proteger un código confidencial de cuatro dígitos - no hace falta decir que esta longitud máxima de cuatro caracteres se da en el presente documento a título puramente ilustrativo, y que esta longitud puede ser fijada en otros valores en otras situaciones). En relación con la figura 6, se presenta un ejemplo de la evolución de una secuencia de este tipo limitada a cuatro caracteres y conservada en la memoria segura asociada al procesador seguro de un dispositivo electrónico de introducción de datos (columna B), consecutivamente a diferentes introducciones de caracteres realizadas por un usuario en este dispositivo (columna A). Los caracteres transmitidos a la aplicación común (AppC) (que, por ejemplo, se ejecutan al nivel del procesador no seguro) se indican en la columna C. En este ejemplo, se considera que el usuario ya ha introducido la secuencia de caracteres «123», después de que haya pulsado sucesivamente las teclas asociadas a los caracteres «4», «5» y «6», en este orden. Desde que se alcanza el tamaño máximo predefinido de la secuencia de caracteres grabada según el procedimiento propuesto registrado, cualquier nueva introducción de carácter conlleva, por una parte, una actualización de la secuencia de caracteres memorizada en los últimos cuatro caracteres introducidos, y, por otra parte, la transmisión inmediata del carácter «liberado» en la aplicación común (AppC) (según el principio bien conocido en informática «primero en entrar, primero en salir» o FIFO en Inglés de «First In, first Out»). Por lo tanto, si estamos interesados en la última línea de la figura 6, la pulsación del usuario sobre la tecla «6» activa una actualización de la secuencia de caracteres mantenida al nivel de la memoria segura asociada al procesador seguro (paso del valor «2345» al valor «3456»), y el fin del almacenamiento del carácter «2», que es transmitido a continuación directamente a la aplicación común (AppC). De esta manera, mientras una validación de una secuencia de caracteres introducida no es detectada por el procesador seguro, solo los cuatro últimos caracteres introducidos son guardados en la memoria asociada al procesador seguro. En lugar de privar a una aplicación común (AppC) de terceros de cualquier retroalimentación después de las introducciones realizadas en el teclado mientras que uno de los pulsadores de validación no ha sido pulsado (almacenamiento, por parte del procesador seguro del conjunto de la secuencia de caracteres introducida mientras no está validada), este modo de realización permite, por consiguiente, transmitirle, a medida que se escriben los caracteres que no forman parte de los cuatro últimos caracteres introducidos (almacenamiento, por parte del procesador seguro, de un número finito de caracteres introducidos de manera única). Imponer una longitud máxima predefinida a la secuencia de caracteres que está guardada en una memoria segura permite asimismo protegerse contra potenciales ataques, lo que conduciría, por ejemplo, a comprometer el procesador seguro saturando la memoria segura que está asociada al mismo, mediante la introducción de una cadena de caracteres de longitud muy importante sin realizar nunca la validación.

Se debe observar que, en otras realizaciones particulares de la técnica propuesta, pulsadores de control distintos de los pulsadores de validación segura y no segura puedan afectar a la secuencia de caracteres registrada en la memoria asociada al procesador seguro. De este modo, los efectos de los pulsadores que permiten corregir o anular una entrada realizada en un dispositivo electrónico de introducción de datos (los pulsadores respectivos (C) y (X) de la figura 2, por ejemplo) se aplican asimismo a la secuencia de caracteres grabada en la memoria segura asociada al procesador seguro. El pulsador de corrección permite de este modo borrar el último carácter de esta secuencia de caracteres. Por lo que respecta al pulsador de anulación, le permite suprimir pura y simplemente dicha secuencia de caracteres de la memoria segura asociada al procesador seguro.

REIVINDICACIONES

1. Procedimiento de protección de una validación de una secuencia de caracteres (SEQ) introducida por un usuario en un dispositivo electrónico de introducción de datos que comprende un procesador no seguro y un procesador seguro, estando dispuesto dicho procesador no seguro bajo el control de dicho procesador seguro, estando realizada dicha introducción en relación con una aplicación común ejecutada por uno de dichos procesadores, estando caracterizado dicho procedimiento por que comprende al nivel de dicho procesador seguro:

- una etapa de obtención de una señal (SIG_V) representativa de un medio de validación, utilizado por dicho usuario para validar dicha secuencia de caracteres (SEQ), siendo emitida dicha señal (SIG_V) por un medio de validación que pertenece a un conjunto que comprende al menos dos medios de validación separados;

- una etapa de obtención, en una memoria segura asociada a dicho procesador seguro, de dicha secuencia de caracteres;

- cuando la señal es representativa de una validación segura, una etapa de comparación de dicha aplicación común con una lista predeterminada de aplicaciones;

  - cuando dicha aplicación común está presente en la lista de predeterminada de aplicaciones:

    - una etapa de transmisión de dicha secuencia de caracteres hacia dicha aplicación común,

    - una etapa de supresión, de dicha memoria segura, de dicha secuencia de caracteres;

  - cuando dicha aplicación común está ausente de la lista predeterminada de aplicaciones, una etapa de supresión, de dicha memoria segura, de dicha secuencia de caracteres.

2. Procedimiento de protección según la reivindicación 1, caracterizado por que comprende, además:

- cuando dicha señal es representativa de una validación no segura:

  - una etapa de transmisión de dicha secuencia de caracteres hacia dicha aplicación común;

  - una etapa de supresión, de dicha memoria segura, de dicha secuencia de caracteres.

3. Procedimiento de protección según una cualquiera de las reivindicaciones 1 a 2, caracterizado por que comprende, además, cuando la aplicación común no está presente en la lista predeterminada de aplicaciones, una etapa de visualización, en una pantalla de dicho dispositivo electrónico de introducción de datos, de un dato representativo de la supresión sin transmisión de dicha secuencia de caracteres.

4. Procedimiento de protección según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que la longitud de dicha secuencia de caracteres, obtenida en dicha memoria segura, está predefinida.

5. Procedimiento de protección según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicha secuencia de caracteres es suprimida de dicha memoria segura si no se realiza ninguna introducción de caracteres en dicho dispositivo electrónico de introducción de datos durante un tiempo predeterminado.

6. Procedimiento de protección según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que dicho dispositivo electrónico de introducción de datos es un terminal de pago.

7. Dispositivo electrónico de introducción de datos que comprende un procesador no seguro y un procesador seguro, estando dispuesto dicho procesador no seguro bajo el control de dicho procesador seguro, estando realizada dicha introducción en relación con una aplicación común ejecutada por uno de dichos procesadores, estando caracterizado dicho dispositivo electrónico de introducción de datos por que comprende:

- un conjunto que comprende al menos dos medios de validación separados;

- medios para determinar, por parte de dicho procesador seguro, un procesamiento a aplicar a dicha secuencia de caracteres, en función de una señal representativa de un medio de validación, utilizada por dicho usuario para validar dicha secuencia de caracteres, siendo emitida dicha señal representativa de una validación por uno de los medios de validación que pertenece a dicho conjunto que comprende al menos dos medios de validación separados.

- medios de obtención, por parte de dicho procesador seguro, de una señal representativa de un medio de validación, utilizada por dicho usuario para validar dicha secuencia de caracteres (SEQ), siendo emitida dicha señal por uno de los medios de validación perteneciente a dicho conjunto que comprende al menos dos medios de validación separados;

- medios de obtención, por parte de dicho procesador seguro, en una memoria segura asociada a dicho procesador seguro, de dicha secuencia de caracteres;

- medios de comparación, por parte de dicho procesador seguro, de dicha aplicación común con una lista predeterminada de aplicaciones, puestos en práctica cuando la señal es representativa de una validación segura;

- medios de transmisión, por parte de dicho procesador seguro, de dicha secuencia de caracteres hacia dicha aplicación común, puestos en práctica cuando dicha aplicación común está presente en la lista predeterminada de aplicaciones;

- medios de supresión, por parte de dicho procesador seguro, de dicha memoria segura, de dicha secuencia de caracteres.

8. Programa informático telecargable desde una red de comunicación y/o almacenado en un medio legible por ordenador y/o ejecutable por un microprocesador, caracterizado por que comprende instrucciones de código de programa para la ejecución de un procedimiento de protección según una cualquiera de las reivindicaciones 1 a 6, cuando es ejecutado en un ordenador.

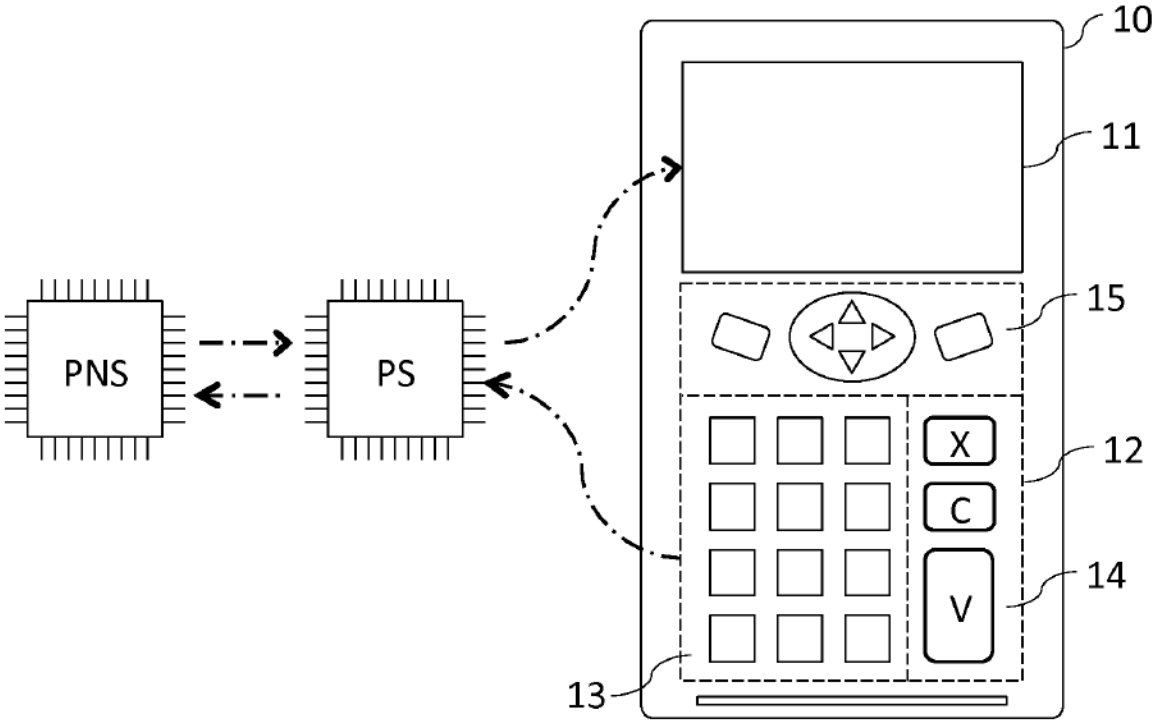

Fig. 1

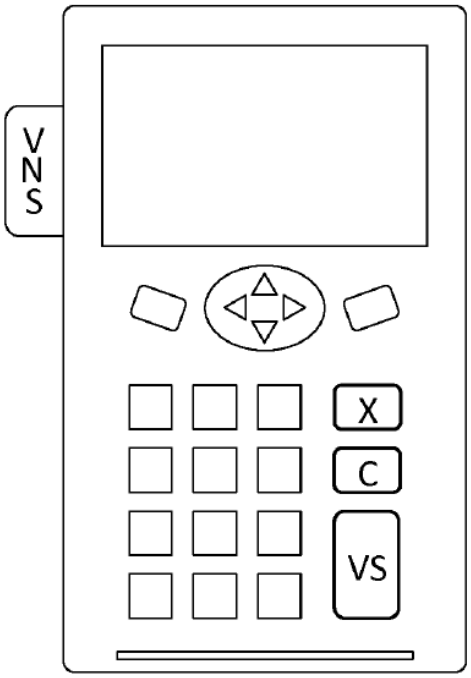

Fig. 2

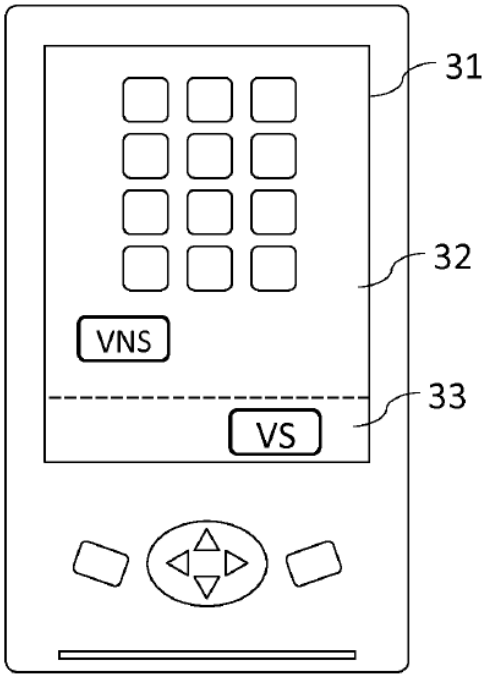

Fig. 3

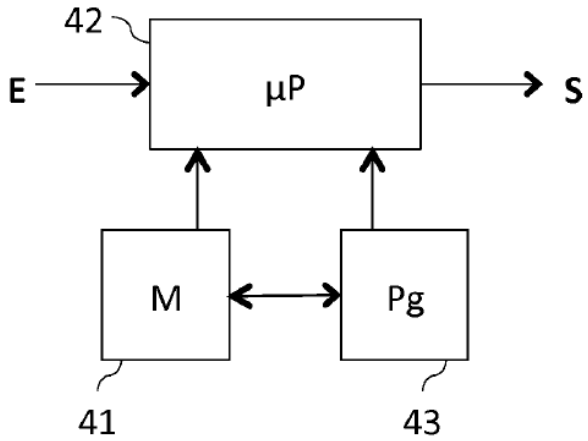

Fig. 4

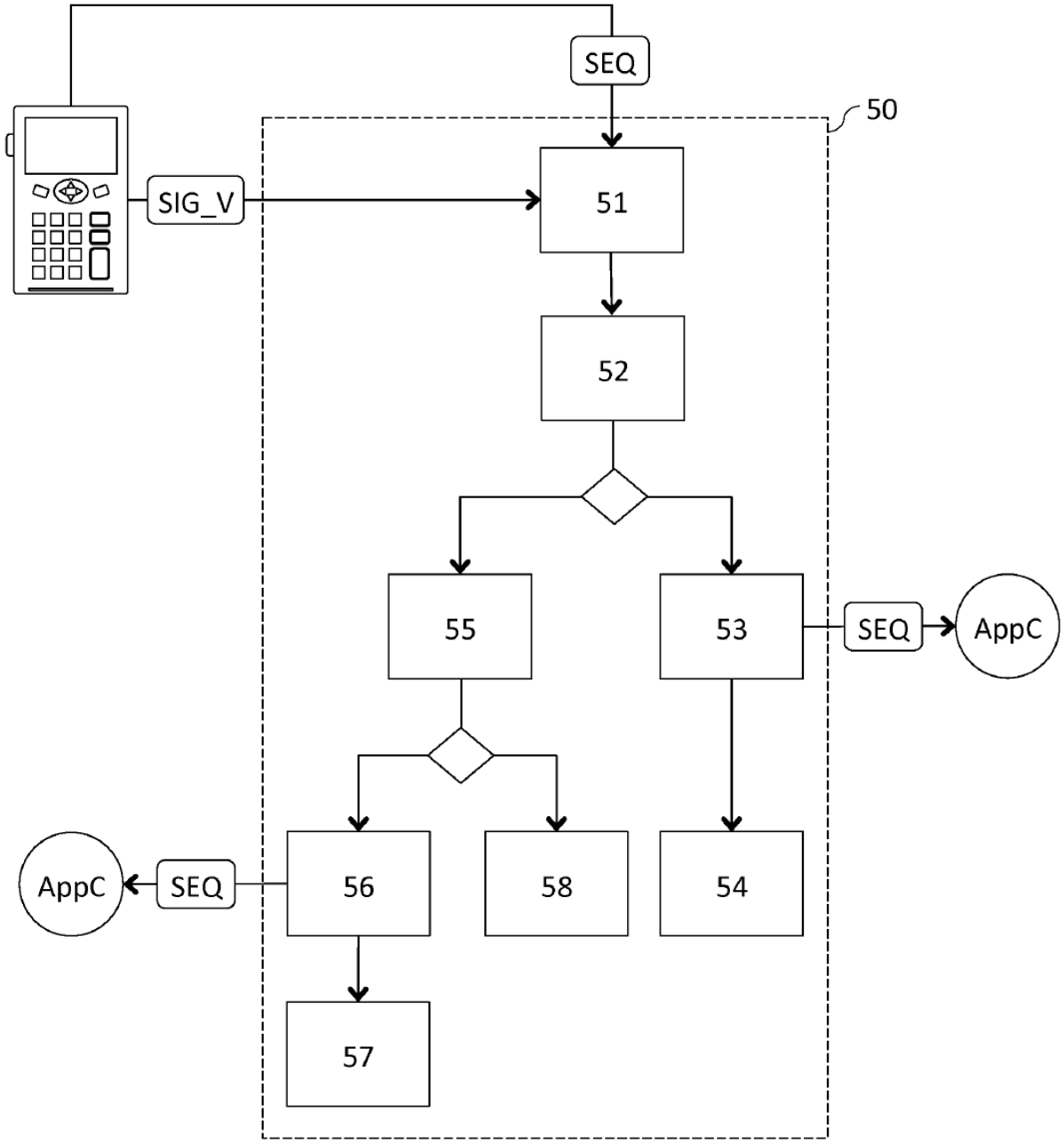

Fig. 5

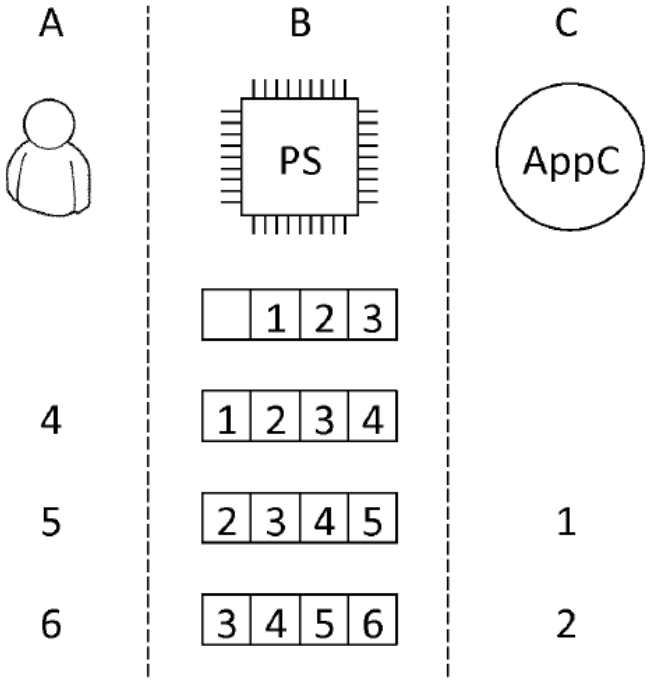

Fig. 6