(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 663 511**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06F 21/34 (2013.01)
G06K 19/073 (2006.01)
G06K 19/077 (2006.01)
G06Q 20/34 (2012.01)
G06Q 20/38 (2012.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.11.2015 E 15195725 (5)**

(97) Fecha y número de publicación de la concesión europea: **03.01.2018 EP 3023926**

(54) Título: **Procedimiento de generación y de visualización de un criptograma para una tarjeta de pago, tarjeta de pago**

(30) Prioridad:

21.11.2014 FR 1461296

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.04.2018

(73) Titular/es:

CB INVESTISSEMENTS (100.0%)
151 bis, rue Saint-Honoré
75001 Paris, FR

(72) Inventor/es:

GAUTIER, SERGE

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Procedimiento de generación y de visualización de un criptograma para una tarjeta de pago, tarjeta de pago

Sector de la técnica

La invención se refiere a una tarjeta de pago provista de un dispositivo de visualización para la visualización de un criptograma para operaciones de verificación de tarjeta dispuesto sobre una cara de la tarjeta de pago, así como un procedimiento de generación y de visualización de un criptograma para tal tarjeta de pago.

La invención se refiere, en particular, al ámbito de las tarjetas bancarias de pago, por ejemplo, de tipo EMV (Europay, Mastercard, Visa) u otro.

Estado de la técnica

Una transacción a distancia con tal tarjeta de pago, por ejemplo, por internet, correo, fax o teléfono, normalmente implica proporcionar un número de cuenta principal PAN inscrito en una cara inscrito en una cara de la tarjeta de pago, así como cierta información adicional, como la fecha de caducidad de la tarjeta de pago y/o la identidad del titular inscrito a la tarjeta.

Con el fin de asegurar la transacción a distancia, además, normalmente es necesario proporcionar un criptograma llamado también valor de verificación de la tarjeta o "CVx2", que el servidor utiliza para operaciones de verificación de la tarjeta. El criptograma normalmente se compone de 3 o 4 cifras inscritas en la tarjeta de pago, en particular, en la cara de la tarjeta que se opone a la cara que lleva el número de cuenta principal PAN.

Las cifras que componen el criptograma, por ejemplo, se determinan cifrando el número de cuenta principal PAN de la tarjeta, su fecha de caducidad, así como un código de servicio de la tarjeta, por una clave numérica única asociada a la tarjeta de pago y, conservando 3 o 4 cifras del resultado obtenido.

En este contexto, se desea impedir la recopilación y/o reutilización de criptogramas por agentes o personas ilegítimas que hubieran tenido acceso a la información de la tarjeta de pago y que hubieran registrado el número de cuenta principal PAN, los datos adicionales y el valor del criptograma.

Para este fin, se han propuesto tarjetas de pago provistas de un dispositivo de visualización de un valor del criptograma, dispuesto sobre una cara de la tarjeta de pago, en las que el valor del criptograma se actualiza periódicamente con el fin de impedir o limitar la reutilización del criptograma por personas ilegítimas.

El documento US 7.954.705 presenta un ejemplo de tal tarjeta de pago y de un procedimiento de generación y de visualización de un criptograma para esta tarjeta de pago.

Los documentos US 2007/136211 A1 y US 2003105964 A1 describen procedimientos según el preámbulo de la reivindicación 1.

Sin embargo, se desea mejorar aún más la seguridad de tales tarjetas de pago, en particular, para prevenir o limitar las posibilidades de implementar una ingeniería de reserva de la tarjeta de pago.

Objeto de la invención

La invención propone un procedimiento de generación y de visualización de un criptograma para una tarjeta de pago que consta de un dispositivo de visualización dispuesto sobre una cara de la tarjeta de pago, comprendiendo el dispositivo de visualización un campo para la visualización de un criptograma para operaciones de verificación de tarjeta realizadas por un servidor de verificación de tarjeta, constando el procedimiento de las operaciones de:

- visualizar, en el campo del dispositivo de visualización, un primer valor del criptograma durante un primer periodo de tiempo,
- visualizar, en el campo del dispositivo de visualización, un segundo valor del criptograma durante un segundo periodo de tiempo después del primer periodo de tiempo, teniendo el primer y el segundo periodo de tiempo duraciones diferentes.

El criptograma se visualiza de este modo en la tarjeta mediante una tinta electrónica u otro tipo de visualización y se actualiza en los intervalos de tiempo calculados. El portador utiliza el valor actual del criptograma de la misma manera que un criptograma permanente no modificable, tal como se utiliza comúnmente hoy en día.

La ganancia en seguridad proviene de la rápida expiración de los números capturados, que debe, por lo tanto, ser ventajosamente bastante rápido para no permitir un uso importante de la tarjeta y, bastante lento para permitir que un usuario asga el criptograma fácilmente.

En particular, si el usuario lee un primer valor del criptograma sobre la tarjeta y después lo transmite al servidor de verificación de tarjeta, mientras que la pantalla de la tarjeta ya ha cambiado a un segundo valor del criptograma, la verificación de la tarjeta puede fallar.

Para reducir el malestar que pueda sentir entonces el usuario de la tarjeta, se puede prever que acepte, en un intervalo de tiempo definido alrededor del momento de cambio de valor, dos valores para el criptograma, siendo estos dos valores en particular, el primer valor y el segundo valor que se siguen temporalmente.

Debido a esto, dicho intervalo de tiempo alrededor del momento de cambio de valor del criptograma es un periodo de tiempo durante el cual, la probabilidad de generar aleatoriamente un criptograma aceptado es dos veces mayor que fuera de este intervalo de tiempo. El procedimiento de generación y de visualización de un criptograma según la invención hace que este intervalo de tiempo sea más difícil de identificar por ingeniería inversa, puesto que los momentos de cambio de valor del criptograma no se siguen periódicamente.

En un modo de realización, una operación de conmutación del primer periodo de tiempo al segundo periodo de tiempo se realiza cuando un contador de tiempo sobrepasa un primer valor de umbral de conmutación asociado con el primer periodo de tiempo, incrementándose el contador de tiempo por un reloj interno de la tarjeta de pago no sincronizado con el servidor de verificación de la tarjeta.

De esta manera, no es posible tener acceso a información de sincronización que indica la conmutación de la tarjeta interceptando los intercambios entre la tarjeta y el servidor de verificación.

Esto permite reforzar la seguridad del criptograma.

Preferentemente, la operación de conmutación del primer periodo de tiempo al segundo periodo de tiempo consta de las etapas de:

- incrementar un contador de valores del criptograma,
- determinar el segundo valor del criptograma que se visualizará durante el segundo periodo de tiempo en función, al menos, de una clave numérica asociada a la tarjeta de pago y del contador de valores del criptograma visualizados,
- actualizar el dispositivo de visualización de la tarjeta para visualizar el segundo valor del criptograma y
- determinar un segundo valor de umbral de conmutación asociado con el segundo periodo de tiempo, en función, al menos, del contador de valores del criptograma visualizados.

En un modo de realización preferido ventajoso, los valores del criptograma visualizados en el campo del dispositivo de visualización no constan de datos de sincronización para el servidor de verificación de la tarjeta.

En un modo de realización particular, el procedimiento consta de una pluralidad de operaciones de visualización sucesivas,
constando cada operación de visualización de la pluralidad de operaciones de visualización la visualización, en el campo del dispositivo de visualización, de un valor del criptograma asociado a dicha operación de visualización durante un periodo de tiempo asociado a dicha operación de visualización,
y los periodos de tiempo sucesivos asociados a las operaciones de visualización sucesivas de la pluralidad de operaciones de visualización forman una serie de no constante calculable.

Preferentemente, un valor de umbral de conmutación asociado a un periodo de tiempo se determina en función del contador de valores del criptograma visualizados, de un valor medio de periodo de tiempo entre dos conmutaciones, de un intervalo de variabilidad único asociado a la tarjeta de pago y de un valor temporal de inicio de funcionamiento de la tarjeta.

Otro aspecto de la presente invención se refiere a una tarjeta de pago que consta de

- un dispositivo de visualización dispuesto sobre una cara de la tarjeta de pago que comprende un campo para la visualización de un criptograma para operaciones de verificación de tarjeta realizadas por un servidor de verificación de tarjeta y
- un circuito de control dispuesto para controlar la visualización, en dicho campo del dispositivo de visualización, al menos de un primer valor del criptograma durante un primer periodo de tiempo y de un segundo valor del criptograma durante un segundo periodo de tiempo después del primer periodo de tiempo, teniendo el primer y el segundo periodo de tiempo duraciones diferentes.

En un modo de realización particular, el circuito de control consta de:

* una memoria para contener un contador de tiempo y, al menos, un valor de umbral de conmutación,
* un reloj interno no sincronizado con el exterior de la tarjeta, para incrementar un contador de tiempo y

* un circuito de control para conmutar del primer periodo de tiempo al segundo periodo de tiempo cuando el contador de tiempo sobrepasa un primer valor de umbral de conmutación asociado al primer periodo de tiempo.

En ese caso, la tarjeta de pago consta ventajosamente, además, de un número de cuenta principal PAN inscrito sobre una cara de la tarjeta de pago.

Otro aspecto de la presente invención se refiere a un programa informático para una tarjeta de pago, el programa consta de instrucciones para implementar las etapas de un procedimiento de generación y de visualización de un criptograma para operaciones de verificación de tarjeta, tales como las descritas anteriormente.

Descripción de las figuras

Otras particularidades y ventajas de la presente invención se pondrán de manifiesto en la descripción a continuación de ejemplos de realización no limitativos, en referencia a los dibujos adjuntos, en los que:

- la figura 1 es un cuadro sinóptico de un sistema de verificación de tarjeta de pago que comprende una tarjeta de pago según la invención, así como un servidor de verificación de tarjeta y una entidad receptora;

- la figura 2 es un cuadro sinóptico detallado de la tarjeta de pago de la figura 1;

- la figura 3 es un diagrama de flujo de operaciones de generación y de visualización de un criptograma para una tarjeta de pago tal como la de las figuras 1 y 2;

- la figura 4 es un diagrama de flujo detallado de una operación de conmutación tal como la realizada durante un procedimiento de generación y de visualización de un criptograma según la invención.

Descripción detallada de la invención

La invención se describe a continuación en su aplicación no limitante a las transacciones a distancia con una tarjeta de tipo EMV (Europay, Mastercard, Visa).

La entidad 1 representada sobre la figura 1 es una tarjeta de pago 1, por ejemplo, una tarjeta de tipo EMV (Europay, Mastercard, Visa).

La entidad 2 es un servidor de verificación de tarjeta que consta al menos de una unidad de entrada 20 de datos de tarjeta y una unidad de tratamiento 21.

La entidad 3 es una entidad receptora 3 con la cual un usuario U de la tarjeta de pago 1 puede comunicarse por un canal de comunicación 4, por ejemplo, por internet, correo, fax o teléfono, en una transacción a distancia con una tarjeta de pago.

La entidad receptora 3 puede ser, de este modo, por ejemplo, un servidor de un sitio web mercantil o de un sitio web de pago en línea o, incluso, un operador que recibe una solicitud de transacción por correo, fax o teléfono. La entidad receptora 3, por lo tanto, es apta para recibir, por canales de comunicación 4 diversos, datos de tarjeta DC de un usuario U de la tarjeta y de pago 1. La entidad receptora 3, además, es apta para transmitirlos al servidor 2 de verificación de la tarjeta por un segundo canal de comunicación 5, por ejemplo, a través de una red, tal como internet, una red intranet o, incluso, una conexión punto a punto cableada o inalámbrica.

La entidad receptora 3 asegura de este modo la mediación entre el usuario U de la tarjeta de pago 1 y el servidor 2 de verificación de la tarjeta.

Los datos de tarjeta DC constan, en particular, de un valor de criptograma C para que la tarjeta de pago 1 lo pruebe, así como de información de identificación ID de dicha tarjeta de pago, por ejemplo, un número de cuenta principal PAN de la tarjeta de pago, una fecha de caducidad de la tarjeta de pago y/o la identidad del titular de la tarjeta de pago.

El servidor de verificación de tarjeta 2 es apta y se destina a implementar operaciones de verificación de tarjeta que constan de, en particular:

- una operación de recepción, por la unidad de entrada 20, de datos de tarjeta.
- Una operación de determinación, por medio de la unidad de tratamiento 21, de un valor de criptograma aceptable. El valor de criptograma aceptable puede, en particular, determinarse a partir de la información de identificación comprendida en los datos de tarjeta, por ejemplo, a partir de un número de cuenta principal PAN, de una fecha de caducidad de la tarjeta de pago y/o de la identidad del titular de la tarjeta de pago. El valor de criptograma aceptable, en particular, se determina sin utilizar el valor de criptograma que se probará comprendido en los datos de la tarjeta.

- Una operación de comparación entre el valor de criptograma que se probará y el valor de criptograma aceptable para determinar si los datos de tarjeta son aceptables.

Durante la operación de determinación de un valor de criptograma aceptable, el servidor de verificación de tarjeta 2 puede ir a buscar en una base de datos 3 información adicional sobre la tarjeta de pago. Esta información adicional puede ser, por ejemplo, valores de semilla para un algoritmo de cálculo de valores de criptograma como se detalla a continuación. La determinación del valor de criptograma aceptable, por lo tanto, se realiza sobre la base de la información de identificación comprendida en los datos de tarjeta, así como de la información adicional obtenida a partir de la base de datos 3.

Dicha base de datos 3 puede asociar dicha información adicional con información de identificación de tarjeta de pago, por ejemplo, números de cuenta primarios PAN, para permitir un acceso fácil a dicha información adicional.

Las operaciones de verificación de tarjeta pueden, por supuesto, constar de operaciones adicionales no mencionadas aquí, por ejemplo, una verificación de la información de identificación de tarjeta de pago, por ejemplo, una verificación del número de cuenta principal PAN de la tarjeta de pago, de la fecha de caducidad de la tarjeta de pago y/o de la identidad del titular de la tarjeta de pago.

Las operaciones de verificación de tarjeta permiten, de manera general, concluir, en la medida de lo posible, en cuanto a la realidad de la posesión de la tarjeta de pago por el usuario U que solicita la transacción a distancia.

La tarjeta de pago 1 es una tarjeta de formato conocido, por ejemplo, tal como se define en las normas ISO 7810 ID-1, ISO 7813, es decir, que presenta, por ejemplo, una forma general de hoja semirrígida fácilmente transportable, con un espesor, por ejemplo, del orden de algunos milímetros y, de algunos centímetros de lado, por ejemplo, constituida por una parte de material plástico.

Consta de dos caras opuestas 1a y 1b. Al menos una de estas caras 1b puede presentar cierto número de información, en particular, información de identificación de tarjeta de pago ID, tal como un número de cuenta principal PAN de la tarjeta de pago, una fecha de caducidad de la tarjeta de pago y/o la identidad del titular de la tarjeta de pago.

Por otra parte, la tarjeta de pago 1 consta de un dispositivo de visualización 10.

El dispositivo de visualización 10 se dispone en una cara 1a de la tarjeta de pago 1. El dispositivo de visualización 10 comprende un campo 10a para la visualización de un criptograma. El dispositivo de visualización 10 se dispone, en particular, sobre una cara 1a de la tarjeta para que el campo 10a pueda estar visible para un usuario de la tarjeta de pago 1.

El dispositivo de visualización 10 puede disponerse sobre la misma cara que cierta información de identificación de la tarjeta de pago. El dispositivo de visualización 10 puede disponerse también sobre una cara 1a, mientras que, la información de identificación de tarjeta de pago se dispone sobre la cara 1b opuesta, para que no sea posible ver al mismo tiempo el criptograma y la información de identificación de tarjeta de pago. Esto reduce el riesgo de fraude.

En un modo de realización que permite la reutilización de los canales de comunicación existentes, los valores del criptograma visualizados en el campo 10a del dispositivo de visualización 10 constan cada uno de 3 o 4 cifras.

La tarjeta de pago 1 consta igualmente de un circuito de control 11, dispuesto para controlar la visualización 200, en el campo 10a del dispositivo de visualización 10 de un valor de criptograma que puede utilizarse para operaciones de verificación de tarjeta realizadas por un servidor de verificación de tarjeta, tal como las descritas anteriormente.

De este modo, en una transacción a distancia con tal tarjeta de pago 1, por ejemplo, por internet, correo, fax o teléfono, el usuario U de la tarjeta puede leer, sobre la tarjeta de pago 1, los datos de tarjeta tales como los detallados anteriormente, es decir, que consta, por ejemplo, del valor de criptograma que se probará, el número de cuenta principal PAN de la tarjeta de pago, la fecha de caducidad de la tarjeta de pago y/o la identidad del titular de la tarjeta de pago y, proporcionar estos datos de tarjeta a la entidad receptora 3 por el canal apropiado (según el modo de realización: entrada de datos en los campos de una página web o de un programa informático, comunicación escrita u oral por carta, faz o teléfono) que los transmite al servidor 2 de verificación de tarjeta para determinar si los datos de tarjeta se aceptan y, si la transacción puede autorizarse.

En un modo de realización, la entidad receptora 3 puede ser directamente el servidor 2 de verificación de tarjeta.

La tarjeta de pago 1 puede constar igualmente de un chip 10 apto para comunicarse eléctricamente o sin contacto con un terminal, en particular, un terminal de pago, para realizar, por ejemplo, operaciones de pago directo tales como se practican con las tarjetas de pago actuales. El circuito de control 11 puede integrarse en el chip 12 o ser un circuito físicamente separado de dicho chip 12.

Por supuesto, en tales operaciones de pago directo, el operador de la tarjeta y el comerciante (máquina mercante o persona física) están en presencia física y, cerca, uno del otro. Por lo tanto, el comerciante normalmente puede confirmar de primera mano o por contacto o detección, la realidad de la posesión de la tarjeta de pago por el usuario que solicita la transacción. La invención se interesa por el caso de transacciones a distancia en el que esta presencia física normalmente no se verifica.

Más particularmente, el circuito de control 11 se dispone para controlar la visualización 200, en el campo 10a del dispositivo de visualización 10, al menos de un primer valor del criptograma C1 durante un primer periodo de tiempo T1 y de un segundo valor del criptograma C2 durante un segundo periodo de tiempo T2 después del primer periodo de tiempo T1.
La figura 3 ilustra un ejemplo de realización de tal procedimiento en el que un bucle 100, 200, 300, 400 permite la visualización sucesiva de los diferentes valores del criptograma. Una operación de conmutación 300 permite pasar de la visualización de un valor del criptograma a la visualización de otro valor del criptograma.

Por otra parte, el esquema funcional presentado en la figura 3 es un ejemplo típico de programa cuyas ciertas instrucciones pueden realizarse con el equipo descrito. Con este fin, la figura 3 puede corresponder al diagrama de flujo del algoritmo general de un programa informático en el sentido de la invención.

Se entiende bien que, en un momento dado, el campo 10a visualiza un único valor de criptograma entre los valores C1 y C2. Este único valor visualizado, sin embargo, es apto para cambiar con el tiempo. En un modo de realización de la invención, el campo 10a, en particular, es apto únicamente para visualizar un solo valor de criptograma en un momento dado y no es apto de visualizar simultáneamente varios valores de criptograma. De esta forma, las dimensiones y el consumo eléctrico del dispositivo de visualización 10 se reducen.

Para este fin, el circuito de control 11 puede constar, en particular, de una memoria 13 y de un reloj interno 14.

La memoria 13 es apta para contener un contador de tiempo CT y, al menos, un valor de umbral de conmutación VS1.

El reloj interno 14 es apto para incrementar dicho contador de tiempo CT a intervalos de tiempo regulares. Ventajosamente, el reloj interno 14 no se sincroniza con el exterior de la tarjeta de pago 1, en particular, no sincronizado con el servidor 2 de verificación de tarjeta. De esta forma, se hace más difícil prever el momento de conmutación entre los diferentes valores de criptograma y el riesgo de fraude se reduce.

Por ejemplo, con este fin, los valores del criptograma visualizados en el campo 10a del dispositivo de visualización 10 no constan de datos de sincronización.

El circuito de control 11 puede, además, constar de un circuito de control 15 y de un circuito de comunicación 16 con el dispositivo de visualización 10.

El circuito de control 15 puede comunicarse con el reloj interno 14, la memoria 13 y el circuito de comunicación 16.

En un modo de realización particular de la invención, el circuito de control 11 puede integrarse en el dispositivo de visualización 10.

En otro modo de realización, el circuito de control 11 y el dispositivo de visualización 10 pueden estar físicamente separados y formar dos chips distintos.

El circuito de control 11 y/o el circuito de control 15 pueden ser, por ejemplo:

- un procesador apto para interpretar instrucciones en forma de programa informático o
- un chip electrónico, en particular, un chip electrónico cuyas etapas del procedimiento de la invención se describen en silicio o incluso
- un chip electrónico programable.

La figura 4 detalla más precisamente las subetapas que pueden estar comprendidas en la operación de conmutación 300.

De este modo, como ya se ve en las figuras 3 y 4, el circuito de control 15 es particularmente apto para implementar, al menos, una operación de conmutación 300 del primer periodo de tiempo T1 al segundo periodo de tiempo T2. Esta operación de conmutación 300 puede, en particular, implementarse cuando el contador de tiempo CT sobrepasa un valor de umbral de conmutación VS1. El valor de umbral de conmutación VS1 puede ser, en particular, un primer valor de umbral de conmutación VS1 asociado al primer periodo de tiempo T1.

Por ejemplo, el contador de tiempo CT se incrementa regularmente 310 por el reloj interno 14 del circuito de control 11 y, cuando dicho contador de tiempo CT sobrepasa un valor umbral definido para cada periodo de tiempo 320, un

nuevo valor del criptograma se visualiza 350 en el campo 10a del dispositivo de visualización 10. En un modo de realización, el contador de tiempo CT puede, entonces, volver a ponerse a cero, o bien, puede determinar un nuevo de umbral teniendo en cuenta el valor ya existente en el contador de tiempo CT.

Más particularmente, la operación de conmutación del primer periodo de tiempo T1 al segundo periodo de tiempo T2 puede constar, al menos, de las etapas de:

- incrementar 330 un contador de valores del criptograma visualizados CV, que consta, por lo tanto, en este caso, del índice i del segundo periodo de tiempo, es decir, el valor 2,
- determinar 340 el segundo valor del criptograma C2 que se visualizará durante el segundo periodo de tiempo T2 en función, al menos, de una clave numérica única M asociada a la tarjeta de pago 1 y del contador de valores del criptograma visualizados CV,
- actualizar 350 el dispositivo de visualización 10 da tarjeta para visualizar el segundo valor del criptograma C2 y
- determinar 360 un segundo valor de umbral de conmutación VS2 asociado al segundo periodo de tiempo T2, en función, al menos, del contador de valores del criptograma visualizados CV.

Se ve que tal algoritmo permite tener fácilmente el primer y el segundo periodo de tiempo T1, T2 de duraciones diferentes.

En un ejemplo de realización, el contador de tiempo CT podrá volver a ponerse a cero durante una etapa adicional de la operación de conmutación.

Por otra parte, estas etapas 310, 320, 330, 340, 350, 360 pueden realizarse, en particular, sucesivamente en el orden anunciado anteriormente. En una posible variante de la invención, las etapas mencionadas anteriormente podrán realizarse en un orden diferente al indicado o, incluso, en paralelo para ciertas o el conjunto de estas etapas.

Para terminar, los diferentes valores del criptograma pueden determinarse por todo el procedimiento de cálculo que permite obtener valores sucesivos calculables, siendo dicho procedimiento de cálculo ventajosamente difícil o imposible de revertir. De este modo, por ejemplo, se puede implementar un algoritmo similar a los algoritmos conocidos de cálculo de criptogramas, por ejemplo, tales como los definidos en las especificaciones EMV (Europay, Mastercard, Visa).

Un tal algoritmo calcula un valor de criptograma en función, en particular, de una clave numérica única M asociada a la tarjeta de pago 1, así como, finalmente, datos de tarjeta, tales como los detallados anteriormente, es decir, por ejemplo, el valor de criptograma que se probará, el número de cuenta principal PAN de la tarjeta de pago, la fecha de caducidad de la tarjeta de pago y/o de la identidad del titular de la tarjeta de pago.

Por lo tanto, para obtener valores sucesivos de criptograma es suficiente con tener en cuenta el contador de valores del criptograma visualizados CV. Para ello, en particular, se puede reemplazar una parte de los valores de entradas de dicho algoritmo por el valor del contador de valores del criptograma visualizados CV, por ejemplo, una parte de dicha clave numérica única M asociada a la tarjeta de pago 1 o, una porción de dichos datos de tarjeta.

Este ejemplo de procedimiento de cálculo del criptograma, por supuesto, se proporciona a título indicativo y no limitante y, las variantes de cálculo de tal serie de valores sucesivos del criptograma son, por supuesto, concebibles.

Se entiende que el procedimiento se adapta particularmente al caso en el que consta de una pluralidad de n operaciones de visualización 200 sucesivas, como se ilustra en la figura 3.

En ese caso, cada operación de visualización i de la pluralidad de operaciones de visualización consta, entonces de la visualización, en el campo 10a del dispositivo de visualización 10, de un valor del criptograma Ci asociado a dicha operación de visualización i durante un periodo de tiempo Ti igualmente asociado a dicha operación de visualización i.

En este caso, por supuesto, el contador de valores del criptograma visualizados CV constará, por ejemplo, sucesivamente de cada valor del índice i de los periodos de tiempo, es decir, sucesivamente los valores que van de 1 a n.

El contador de valores del criptograma visualizados CV permite, entonces, memorizar el índice i del valor del criptograma actualmente visualizado. Para simplificar la comprensión de la invención, en la presente descripción, se utilizará el índice i para referirse al índice del valor del criptograma actualmente visualizado, teniendo en cuenta que dicho valor es en la práctica para contenerse en la variable CV actualizada durante la implementación del procedimiento según la invención.

Como se detallará ahora, los periodos de tiempo sucesivos T1, …, Tn asociados a las operaciones de visualización sucesivas de la pluralidad de operaciones de visualización pueden formar una serie no constante calculable.

Por "serie no constante", se entiende, en particular, que al menos dos periodos de tiempo Ti, Tj, entre la pluralidad de periodos de tiempo sucesivos T1, …, Tn, presentan duraciones diferentes entre sí. En otras palabras, se entiende que la conmutación del dispositivo de visualización 10 no es periódica en el tiempo.

Ventajosamente, una mayoría de los periodos de tiempo sucesivos T1, …, Tn, pueden ser distintos entre sí, incluso todos los periodos de tiempo sucesivos T1, …, Tn, pueden ser diferentes entre sí, ningún periodo de tiempo T1, …, Tn sin presentar la misma duración que otro periodo de tiempo T1, …, Tn.

Por "serie calculable", se entiende, en particular, que la continuación de los periodos de tiempo sucesivos T1, …, Tn es predecible y puede calcularse a partir de un conjunto de datos predefinido y conocido, por ejemplo, del fabricante de la tarjeta de pago.

En particular, por lo tanto, no es posible que el servidor 2 de verificación de tarjeta verifique el valor actual visualizado en el criptograma sin necesitar intercambiar información de sincronización con la tarjeta de pago 1.

Dicho conjunto de datos predefinido se conoce y puede constar, en particular, del número de cuenta principal PAN, la fecha de caducidad de la tarjeta de pago y/o de la identidad del titular de la tarjeta de pago, pero también, de los valores de semilla para un algoritmo de cálculo de valores de criptograma como se detallará a continuación en un modo particular de un procedimiento según la invención.

De este modo, por ejemplo, se puede determinar una variación TVARi asociada a un periodo de tiempo Ti, por ejemplo, de la siguiente manera, en función del contador de valores del criptograma visualizados CV, que vale, en este ejemplo i, y de un intervalo de variabilidad único asociado a la tarjeta de pago PVAR:

$$TVAR_i = i^2 \bmod PVAR$$

Un valor de umbral de conmutación VSi asociado a un periodo de tiempo Ti puede, entonces, determinarse en función de la variación TVARi asociada al periodo de tiempo Ti, así como de un valor medio de periodo de tiempo entre dos conmutaciones VSm y de un valor temporal de inicio de funcionamiento de la tarjeta T0, por ejemplo, como:

$$VS_i = T0 + i * VSm + TVAR_i$$

De esta manera, el valor de umbral de conmutación VSi asociado al periodo de tiempo Ti se determina y es calculable sin sincronización por la tarjeta y el servidor.

Ventajosamente, la variación entre los valores sucesivos de umbral de conmutación VSi es en sí misma no periódica, es decir, la variación de duración de la continuación de los periodos de tiempo sucesivos T1, …, Tn es no periódica y, por lo tanto, no es fácilmente predecible.

Cabe destacar que esto va más allá de la simple no periodicidad de los momentos de conmutación del dispositivo de visualización 10, puesto que, esta es la ausencia de periodicidad (es decir, la variación entre los periodos de tiempo Ti, Ti+1 sucesivos) que es en sí misma no periódica.

En este modo de realización particular, los valores de semilla son, en particular, el valor medio de periodo de tiempo entre dos conmutaciones VSm, el intervalo de variabilidad único asociado a la tarjeta de pago PVAR y el valor temporal de inicio de funcionamiento de la tarjeta T0.

Se entiende, por lo tanto, que estos valores de semilla pueden compartirse fácilmente entre la tarjeta de pago 1 y el servidor 2 de verificación de tarjeta, por ejemplo, durante, o justo después de, la fabricación de la tarjeta de pago 1.

Además, la serie de valores de umbral de conmutación VSi asociada a un periodo de tiempo Ti es, por lo tanto, una serie no constante calculable. Por lo tanto, la serie de periodos de tiempo sucesivos Ti, asociados a las operaciones de visualización sucesivas i de la pluralidad de operaciones de visualización forman también una serie no constante calculable.

Los diferentes valores de semilla se seleccionan para asegurar una variabilidad suficiente a la serie de periodos de tiempo sucesivos Ti para reducir el riesgo de fraude, mientras se conserva una utilización fácil para el operador, es decir, garantizando un tiempo de visualización suficiente de cada valor del criptograma para permitir una lectura y una recogida a una velocidad normal para el usuario.

Por supuesto, se entiende que las ecuaciones anteriores, que permiten determinar el valor de umbral de conmutación VSi asociado a un periodo de tiempo Ti, se proporcionan únicamente a título de ejemplo no limitante.

De este modo, se puede considerar modificar la forma exacta de estas ecuaciones y utilizar valores de semilla adicionales, tales como un paso de tiempo definido, por ejemplo, para asegurar un tiempo mínimo de visualización de cada valor del criptograma.

Por supuesto, la presente invención no se limita a las formas de realización descritas anteriormente a título de ejemplo; se extienden a otras variantes.

Son posibles otras realizaciones.

REIVINDICACIONES

1. Procedimiento de generación y de visualización de un criptograma para una tarjeta de pago (1) que consta de un dispositivo de visualización (10) dispuesto sobre una cara (1a) de la tarjeta de pago, comprendiendo el dispositivo de visualización un campo (10a) para la visualización de un criptograma para operaciones de verificación de tarjeta realizadas por un servidor (2) de verificación de tarjeta, constando el procedimiento de las operaciones de:

- visualizar (200), en el campo del dispositivo de visualización, un primer valor del criptograma (C1) durante un primer periodo de tiempo (T1),
- visualizar, en el campo del dispositivo de visualización, un segundo valor del criptograma (C2) durante un segundo periodo de tiempo (T2) después del primer periodo de tiempo,

el procedimiento **caracterizándose por que** el primer y el segundo periodo de tiempo tienen duraciones diferentes.

2. Procedimiento según la reivindicación 1, en el que una operación de conmutación (300) del primer periodo de tiempo (T1) al segundo periodo de tiempo (T2) se realiza cuando un contador de tiempo (CT) sobrepasa un primer valor de umbral de conmutación (VS1) asociado con el primer periodo de tiempo (T1), incrementándose el contador de tiempo por un reloj interno (14) de la tarjeta de pago (1) no sincronizado con el servidor (2) de verificación de la tarjeta.

3. Procedimiento según la reivindicación 2, en el que la operación de conmutación (300) del primer periodo de tiempo (T1) al segundo periodo de tiempo (T2) consta de las etapas de:

- incrementar (330) un contador de valores del criptograma visualizados (CV),
- determinar (340) el segundo valor del criptograma (C2) que se visualizará durante el segundo periodo de tiempo (T2) en función, al menos, de una clave numérica única (M) asociada a la tarjeta de pago (1) y del contador de valores del criptograma visualizados (CV),
- actualizar (350) el dispositivo de visualización (10) de la tarjeta para visualizar el segundo valor del criptograma (C2) y
- determinar (360) un segundo valor de umbral de conmutación (VS2) asociado al segundo periodo de tiempo, en función, al menos, del contador de valores del criptograma visualizados (CV).

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, en el que los valores del criptograma (C1, C2) visualizados en el campo (10a) del dispositivo de visualización (10) no constan de datos de sincronización para el servidor (2) de verificación de la tarjeta.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, que consta de una pluralidad de n operaciones de visualización (200) sucesivas,
cada operación de visualización i, entre la pluralidad de n operaciones de visualización, constando de la visualización, en el campo (10a) del dispositivo de visualización (10), de un valor del criptograma (Ci) asociado a dicha operación de visualización durante un periodo de tiempo (Ti) asociado a dicha operación de visualización,
y en el que los periodos de tiempo (Ti) sucesivos asociados a las operaciones de visualización sucesivas de la pluralidad de n operaciones de visualización forman una serie de no constante calculable.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, en el que un valor de umbral de conmutación (VSi) asociado a un periodo de tiempo (Ti) se determina en función del contador de valores del criptograma visualizados (CV), de un valor medio de periodo de tiempo entre dos conmutaciones (VSm), de un intervalo de variabilidad único asociado a la tarjeta de pago (PVAR) y de un valor temporal de inicio de funcionamiento de la tarjeta (T0).

7. Tarjeta de pago (1) que consta de

- un dispositivo de visualización (10) dispuesto sobre una cara (1a) de la tarjeta de pago que comprende un campo (10a) para la visualización de un criptograma para operaciones de verificación de tarjeta realizadas por un servidor (2) de verificación de tarjeta y
- un circuito de control (11) dispuesto para controlar la visualización, en dicho campo del dispositivo de visualización, al menos de un primer valor del criptograma (C1) durante un primer periodo de tiempo (T1) y de un segundo valor del criptograma (C2) durante un segundo periodo de tiempo (T2) después del primer periodo de tiempo,

caracterizado por que el primer y el segundo periodo de tiempo tienen duraciones diferentes.

8. Tarjeta de pago (1) según la reivindicación 7, en la que el circuito de control (11) consta de:

* una memoria (13) para contener un contador de tiempo (CT) y, al menos, un valor de umbral de conmutación (VSi),

* un reloj interno (14) no sincronizado con el exterior de la tarjeta, para incrementar el contador de tiempo y
* un circuito de tratamiento (15) para conmutar del primer periodo de tiempo (T1) al segundo periodo de tiempo (T2) cuando el contador de tiempo sobrepasa un primer valor de umbral de conmutación (VS1) asociado al primer periodo de tiempo (T1).

9. Tarjeta de pago (1) según la reivindicación 8, que consta, además, de un número de cuenta principal PAN inscrito sobre una cara (1b) de la tarjeta de pago.

10. Programa informático para una tarjeta de pago (1), comprendiendo el programa instrucciones para implementar las etapas de un procedimiento de generación y de visualización de un criptograma para operaciones de verificación de tarjeta, según una de las reivindicaciones 1 a 6.

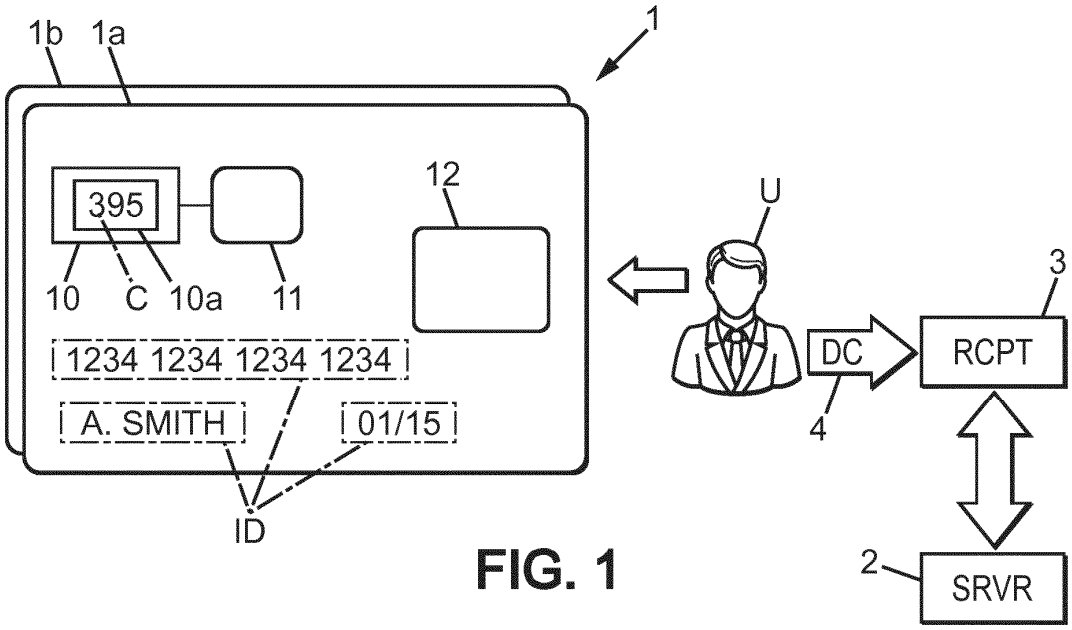
1b
1a
1
395
12
U
3
10
C
10a
11
DC
RCPT
1234 1234 1234 1234
4
A. SMITH
01/15
ID
2
SRVR

FIG. 1

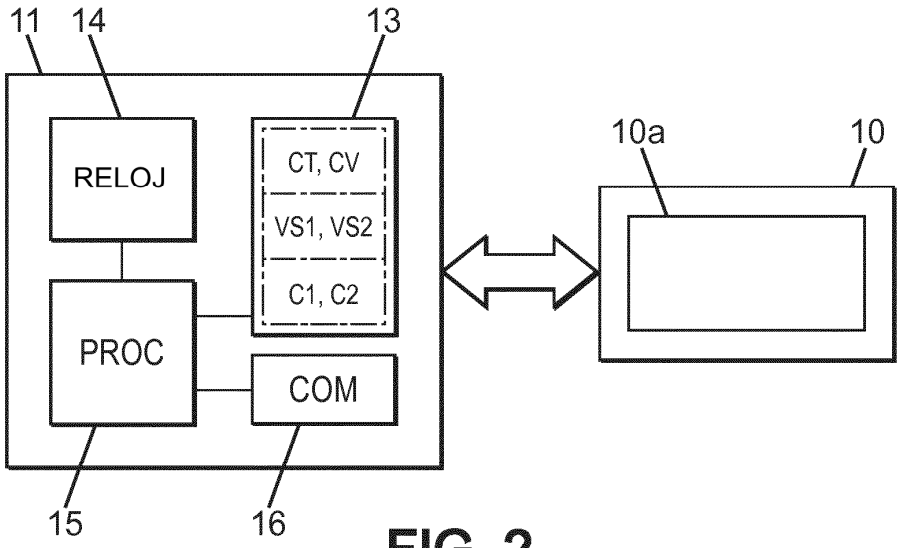
11
14
13
10a
10
RELOJ
CT, CV
VS1, VS2
C1, C2
PROC
COM
15
16

FIG. 2

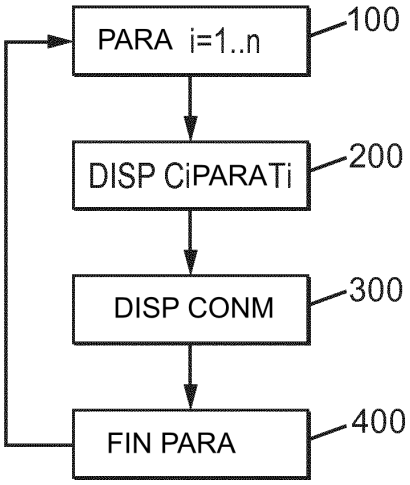
PARA i=1..n
100
DISP CiPARATi
200
DISP CONM
300
FIN PARA
400

FIG. 3

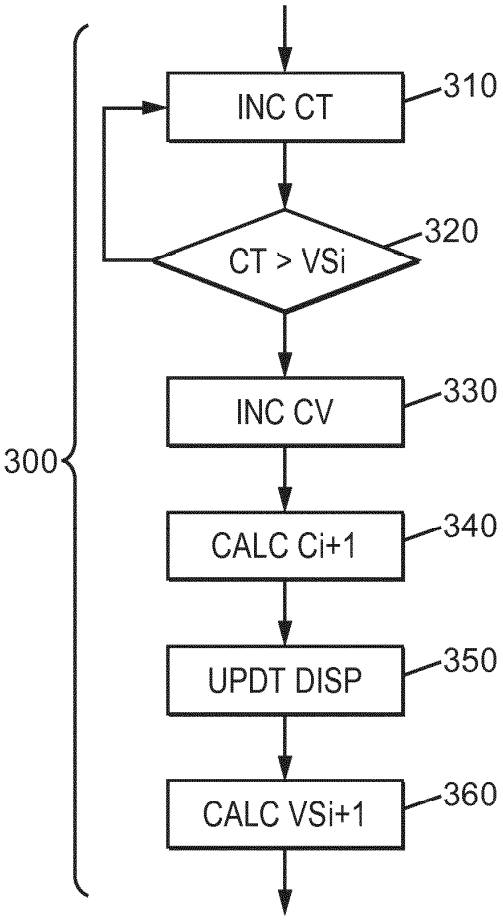
INC CT
310
CT > VSi
320
INC CV
330
300
CALC Ci+1
340
UPDT DISP
350
CALC VSi+1
360

FIG. 4