

Señor

**DIRECTOR DIVISIÓN DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

E. S. D.

REF: Expediente No. **NC2021/0000053**, solicitud de patente de invención a favor de **YOUTRANSACTOR**, Título: **MÉTODO PARA PROTEGER UN TERMINAL DE PAGO**

RESPUESTA A EXAMEN DE FONDO

JUAN PABLO CADENA SARMIENTO, portador de la tarjeta profesional No. 57.492 del C.S.J., obrando como apoderado de la sociedad solicitante me permito dar respuesta al Oficio No. 12372 relacionado con la patentabilidad de la presente invención y notificado el 17 de julio de 2024.

En respuesta a las observaciones realizadas como resultado del examen de fondo, es pertinente mencionar que las reivindicaciones cumplen a cabalidad con los requerimientos de patentabilidad establecidos en la Decisión 486 de 2000, razón por la que respetuosamente disiento de los comentarios del Examinador a este respecto. A continuación, sin embargo, se presentan argumentos y se mencionan las modificaciones realizadas para atender a cada uno de los requerimientos del Examinador:

1. Modificación a las reivindicaciones

Me permito dirigir la atención del Señor Examinador en el hecho que el Capítulo Reivindicatorio adjunto al presente memorial ha sido modificado de la siguiente manera:



- Las antiguas reivindicaciones 2, 5 y 7 han sido eliminadas del Capítulo Reivindicatorio Modificado y, por lo tanto, la numeración y dependencia de las reivindicaciones ha sido modificada de conformidad con las eliminaciones mencionadas.
- La reivindicación 1 ha sido modificada incluyendo las características de las antiguas reivindicaciones 2, 5 y 7 con el fin de definir el “segundo reloj”, “el período de ejecución T1” y la “pluralidad de claves”.
- La antigua reivindicación independiente 13 (nueva reivindicación independiente 10) ha sido modificada incluyendo las características de la reivindicación 1 y así superar las objeciones del examinador.
- Hemos modificado la traducción de la versión original PCT de la característica de la reivindicación 1 une clé (MK) de cryptage de données accédée pour le cryptage de données à sécuriser por una clave (MK) de cifrado de datos a la que se accede para cifrar los datos que se van a proteger ya que es una traducción mucho más adecuada.

Así las cosas, es importante mencionar que las modificaciones realizadas a las reivindicaciones cumplen en su totalidad con los requisitos establecidos en el Artículo 34 de la Decisión 486, teniendo en cuenta que estas **no involucran una ampliación a la protección correspondiente a la divulgación tal y como se presentó originalmente**. Por el contrario, el Capítulo Reivindicatorio Modificado y adjunto al presente memorial cumple con los lineamientos establecidos por la Decisión Andina 486 y encuentra sustento a lo largo de la memoria descriptiva de la solicitud.

2. Unidad de Invención

El examinador establece que “Conforme a lo establecido por el artículo 25 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la solicitud no cumple con el requisito de unidad de invención debido a que se refiere a 2 grupos inventivos”.

Además, indica que los grupos inventivos están definidos por las siguientes características esenciales:

Grupo inventivo 1: Un método (100) para proteger un terminal de pago (reivindicaciones 1 a 12).

Grupo inventivo 2: Un terminal (1) de pago seguro (reivindicación 13).

En respuesta a lo anterior, se presenta un nuevo Capítulo Reivindicatorio en el que la antigua reivindicación 13 (nueva reivindicación 10) se modificó incluyendo las características y restricciones de la reivindicación 1 por lo que ahora comparten el mismo concepto inventivo.

De esta manera, amablemente solicito retirar las objeciones al respecto, ya que la invención cumple con todos los requerimientos dispuestos en el Artículo 25 de la Decisión 486 de 2000.

De acuerdo con lo anteriormente expuesto, respetuosamente solicito el retiro de las objeciones de la presente solicitud y la concesión del privilegio solicitado, ya que en opinión del solicitante cumple con todos los requisitos establecidos en la Decisión 486.

3. Anexos

- Capítulo Reivindicatorio Modificado
- Tasa Oficial

JUAN PABLO CADENA SARMIENTO

T.P. No. 57.492 del C.S.J.
C.C. 80.410.337 de Usaquén
Calle 70 A No. 4 – 41



REIVINDICACIONES

1. Un método (100) para proteger un terminal de pago (1), comprendiendo dicho terminal de pago (1):

- una clave (MK) de cifrado de datos a la que se accede para cifrar los datos que se van a proteger, siendo la clave (MK) de cifrado generada mediante la combinación de una pluralidad de claves (K1, K2) almacenadas en por lo menos una memoria (151, 152) del terminal (1);
- un módulo (120) de vigilancia de por lo menos un parámetro físico del terminal que comprende un medio de medición de dicho parámetro físico;
- un microcontrolador (10);
- una unidad de contador de microcontrolador,
- un primer reloj (LSI), estando la unidad de contador subordinada a dicho primer reloj para incrementar a intervalos regulares un valor de contador de la unidad de contador;

dicho método comprendiendo las siguientes etapas:

- (E10a) medición de un parámetro físico por el medio de medición del dispositivo de vigilancia;
- (E10b) comparación del valor medido con un valor umbral predeterminado, correspondiente a un ataque físico a dicho terminal por parte del dispositivo de vigilancia;
- (E11) eliminación del acceso a la clave (MK) de cifrado de datos por parte del microprocesador (10) si se cumple una de las siguientes condiciones:

por lo menos un valor de parámetros físicos es significativo de un ataque físico a dicho terminal;

el valor de contador es mayor que un valor umbral predefinido;

- (E13) reinicio de la unidad de contador por el dispositivo de vigilancia;

en donde las etapas de medición (E10a), comparación (E10b) y reinicio (E13) se ejecutan periódicamente de acuerdo con un período de ejecución T1 que se encuentra aleatoriamente en un intervalo de valores predefinidos [T1a; T1b];

en el que el terminal (1) también comprende:

- un segundo reloj (LSE) con una frecuencia predefinida para controlar el período de ejecución T1, estando configurado dicho reloj (LSE) para transmitir en una etapa (E0) una interrupción al microcontrolador para la

ejecución periódica de las etapas de medición (E10a), de comparación (E10b) y de reinicio (E13); y

- un tercer reloj (HSI) con una frecuencia predefinida; y

en donde el método (100) incluye una etapa de verificación de la frecuencia del segundo reloj que comprende:

- incrementar una unidad de contador en cada señal de reloj del segundo reloj;
- determinar una frecuencia calculando el número de incrementos en un ciclo de reloj del tercer reloj;
- comparar la frecuencia calculada con un intervalo de frecuencia predeterminado; y si la frecuencia calculada no está dentro del intervalo
- suprimir por lo menos una clave de la pluralidad de claves.

2. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 1, en donde la pluralidad de claves (K1, K2) comprende una primera clave (K1) y una segunda clave (K2), almacenándose la primera clave (K1) en una zona de memoria (151) de tipo registro de microprocesador (10), almacenándose la segunda clave (K2) en una zona de memoria (152) de tipo de memoria volátil del microprocesador (10), y en el que la etapa de borrado (E11) comprende el borrado de por lo menos una clave de la zona de memoria asociada.
3. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 2, en el que la etapa de borrado (E11) implementa distintos métodos de borrado para la primera clave (K1) almacenada en una zona de memoria (151) de tipo registro del microprocesador (10), y la segunda clave (K2) almacenada en una zona de memoria (152) del tipo de memoria volátil del microprocesador (10).
4. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 1, en el que el método (100) también comprende las siguientes etapas:
 - verificar que el valor del período de ejecución T1 está dentro de un intervalo de valores predefinido, y si el valor no está dentro del intervalo:
 - suprimir por lo menos una clave de la pluralidad de claves.
5. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 1, en el que el terminal también incluye una etapa (E30) de verificación de la frecuencia del tercer reloj (HSI) que comprende:

- incrementar una unidad de contador para cada señal de reloj del tercer reloj (HSI);
 - determinar una frecuencia calculando el número de incrementos en un ciclo de reloj del primer reloj (LSI);
 - comparar la frecuencia calculada con un intervalo de frecuencia predeterminado; y si la frecuencia calculada no está dentro del intervalo, suprimir por lo menos una clave de la pluralidad de claves.
6. El método (100) para proteger un terminal de pago (1) de acuerdo con la reivindicación 1, en el que el terminal (1) también comprende un filtro de paso de banda configurado para filtrar una banda de frecuencias predefinidas y para recibir una señal de reloj del primer reloj (LSI), y dicho método (100) también incluye una etapa que comprende eliminar por lo menos una clave de la pluralidad de claves si no hay señal presente en la salida del filtro.
7. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 1, en el que el dispositivo (120) de vigilancia de por lo menos un parámetro físico del terminal (1) comprende uno o más medios de medición configurados para:
- medir el voltaje de alimentación del terminal de pago (1);
 - medir la temperatura de funcionamiento del terminal de pago (1);
 - detectar la apertura del terminal de pago (1); y
 - detectar la perforación del terminal de pago (1).
8. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 1, en el que el dispositivo de vigilancia (120) está configurado para emitir una señal de violación (S1) significativo de un ataque físico a dicho terminal; y en el que el microcontrolador (10) comprende por lo menos un puerto de recepción de dicha señal de violación (S1); y en el que el acceso a la clave (MK) de cifrado de datos se elimina al recibir dicha señal (S1) en dicho puerto de recepción.
9. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 8, en el que el microprocesador (10) también está configurado para, previo a la eliminación del acceso a la clave (MK) de cifrado de datos, ejecute un algoritmo de filtro después de recibir la señal de violación (S1), detectando dicho algoritmo de filtrado si la señal de violación (S1) es significativa de un ataque físico a dicho terminal, y en este caso proceder con el borrado (E11) del acceso a la clave (MK) de cifrado de datos.

10. Un terminal (1) de pago seguro compuesto por:

- una clave de cifrado de datos a la que se accede para cifrar los datos que se van a proteger, siendo la clave (MK) de cifrado generada mediante la combinación de una pluralidad de claves (K1, K2) almacenadas en por lo menos una memoria (151, 152) del terminal (1);
- un dispositivo (120) para vigilar por lo menos un parámetro físico del terminal que comprende un medio de medición dicho parámetro físico;
- un microcontrolador (10);
- una unidad de contador del microcontrolador (10),
- un primer reloj (LSI), estando la unidad de contador subordinada a dicho primer reloj (LSI) para incrementar a intervalos regulares un valor de contador de la unidad de contador;

dicho dispositivo de vigilancia (120) está configurado para periódicamente ejecutar las siguientes etapas de acuerdo con un período de ejecución T1 que se encuentra aleatoriamente en un intervalo de valores predefinidos [T1a; T1b]:

(E10a) medir un parámetro físico por los medios de medición;

(E10b) comparar el valor medido con un valor umbral predeterminado, correspondiente a un ataque físico a dicho terminal por parte del dispositivo de vigilancia (120);

(E11) eliminar el acceso a la clave (MK) de cifrado de datos si se cumple una de las siguientes condiciones:

por lo menos un valor de los parámetros físicos es significativo de un ataque físico a dicho terminal;

el valor de contador es mayor que un valor umbral predefinido;

y;

(E 13) reiniciar la unidad de contador;

en donde el terminal (1) de pago seguro también comprende:

- un segundo reloj (LSE) con una frecuencia predefinida para controlar el período de ejecución T1, estando configurado dicho reloj (LSE) para transmitir en una etapa (E0) una interrupción al microcontrolador para la ejecución periódica de las etapas de medir (E10a), comparar (E10b) y reiniciar (E13); y
- un tercer reloj (HSI) con una frecuencia predefinida; y

en el que dicho dispositivo de vigilancia (120) está configurado además para realizar una etapa (E50) de verificación de la frecuencia del segundo reloj (LSE) que comprende:

incrementar una unidad de contador en cada señal de reloj del segundo reloj;

determinar una frecuencia calculando el número de incrementos en un ciclo de reloj del tercer reloj;

comparar la frecuencia calculada con un intervalo de frecuencia predeterminado; y si la frecuencia calculada no es el intervalo

suprimir por lo menos una clave de la pluralidad de claves.