

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 por cifrado de datos para asegurar;
- 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 reloj (LSI), estando la unidad de contador subordinada a dicho reloj para incrementar a intervalos regulares un valor de contador de la unidad de contador;

dicho método comprende 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) supresión del acceso a la clave (MK) de cifrado de datos por parte del microprocesador (10) si se cumple una de las siguientes condiciones:

- o por lo menos un valor de parámetros físicos es significativo de un ataque físico a dicho terminal;
 - o el valor de contador es mayor que un valor umbral predefinido;
 - (E13) reinicio de la unidad de contador por el dispositivo de vigilancia; y en el que las etapas de medición (E10a), de comparación (E10b) y de reinicio (E13) se ejecutan periódicamente.
2. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 1 en el que la clave (MK) de cifrado se genera mediante la combinación de una pluralidad de claves (K1, K2) almacenadas en por lo menos una memoria (151, 152) del terminal (1).
 3. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 2 en el que la clave (MK) de cifrado se genera mediante la combinación de 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.
 4. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación 3 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).

5. El método (100) para proteger un terminal de pago (1) de acuerdo con una de las reivindicaciones anteriores, en el que el período de ejecución T1 se incluye aleatoriamente en un intervalo de valores predefinidos [T1a; T1b].
6. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación anterior, en el que el método (100) también comprende las siguientes etapas:
 - verificación de que el valor del retardo predefinido T1 está incluido en un intervalo de valores predefinido, y si el valor no está incluido en el intervalo:
 - supresión de por lo menos una clave de la pluralidad de claves.
7. El método (100) para proteger un terminal de pago (1) de acuerdo con una de las reivindicaciones 5 a 6, en el que el terminal de pago (1) también incluye 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).

8. El método (100) para proteger un terminal de pago (1) de acuerdo con la reivindicación anterior, en el que el terminal (1) también comprende un tercer reloj (HSI) con una frecuencia predefinida y en el que el método (100) comprende una etapa (E50) de verificación de la frecuencia del segundo reloj (LSE) comprendiendo:
- el incremento de una unidad de contador en cada señal de reloj del segundo reloj;
 - la determinación de una frecuencia calculando el número de incrementos en un ciclo de reloj del tercer reloj;
 - la comparación de la frecuencia calculada con un intervalo de frecuencia predeterminado; y si la frecuencia calculada no es el intervalo
 - la supresión de por lo menos una clave de la pluralidad de claves.
9. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación anterior en el que el terminal también incluye una etapa (E30) de verificación de la frecuencia del tercer reloj (HSI) que comprende:
- el incremento de una unidad de contador para cada señal de reloj del tercer reloj (HSI);
 - la determinación de una frecuencia calculando el número de incrementos en un ciclo de reloj del primer reloj (LSI);
 - la comparación de la frecuencia calculada con un intervalo de frecuencia predeterminado; y si la frecuencia calculada no es el intervalo
 - la supresión de por lo menos una clave de la pluralidad de claves.

10. El método (100) para proteger un terminal de pago (1) de acuerdo con una de las reivindicaciones anteriores, 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.
11. El método (100) para proteger un terminal de pago (1), de acuerdo con una de las reivindicaciones anteriores, 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).
12. El método (100) para proteger un terminal de pago (1), de acuerdo con una de las reivindicaciones anteriores, 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 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.

13. El método (100) para proteger un terminal de pago (1), de acuerdo con la reivindicación anterior, 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.

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

- una clave (MK) de cifrado de datos, accediéndose a dicha clave (MK) de cifrado por el cifrado de datos a asegurar;
- 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 reloj (LSI), estando la unidad de contador subordinada a dicho 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:
- (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:
 - o por lo menos un valor de los parámetros físicos es significativo de un ataque físico a dicho terminal;
 - o el valor de contador es mayor que un valor umbral predefinido;y;
- (E 13) reiniciar la unidad de contador.

15. Un producto de programa informático que comprende instrucciones de código para la ejecución de un método (100) para proteger un terminal de pago (1) de acuerdo con cualquiera de las reivindicaciones 1 a 13 cuando se ejecuta este programa por un procesador.