(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 641 265**

(51) Int. CI.:

G07F 7/10 (2006.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.08.2007 PCT/EP2007/058834**

(87) Fecha y número de publicación internacional: **28.02.2008 WO08023065**

(96) Fecha de presentación y número de la solicitud europea: **24.08.2007 E 07802879 (2)**

(97) Fecha y número de publicación de la concesión europea: **28.06.2017 EP 2054862**

(54) Título: **Procedimiento de personalización de un componente de seguridad, en concreto, en medio no protegido**

(30) Prioridad:

25.08.2006 FR 0607524

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.11.2017

(73) Titular/es:

THALES (100.0%)
Tour Carpe Diem, Place des Corolles, Esplanade Nord
Courbevoie, FR

(72) Inventor/es:

D'ATHIS, THIERRY;
DAILLY, PHILIPPE y
RATIER, DENIS

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de personalización de un componente de seguridad, en concreto, en medio no protegido

La invención se refiere a un procedimiento de personalización de un componente de seguridad en medio no protegido. En particular, la invención se aplica a los componentes de tipo módulo de acceso seguro (o según la expresión anglosajona Security Access Module).

Los componentes de tipo módulo de acceso seguro se utilizan en numerosos sistemas, por ejemplo, dentro de sistemas de billetes. Estos sistemas implementan, con la ayuda de estos componentes, unos procedimientos criptográficos que cumplen, en concreto, unas funciones de cifrado/descifrado, de autentificación, de colocación de firmas... Estos diferentes procedimientos criptográficos, sea cual sea la tecnología empleada, necesitan, al menos en su fase de inicialización, un primer secreto (clave simétrica, clave asimétrica, aleatoria...). Ahora bien, del nivel de confidencialidad de este primer secreto depende el nivel de seguridad de las funciones de seguridad del sistema. En efecto, el compromiso de este primer secreto conlleva generalmente una pérdida de confianza con respecto al conjunto de la cadena de seguridad que depende de este primer secreto.

La introducción de un primer secreto dentro de un componente de seguridad se lleva a cabo generalmente por el fabricante de dicho componente. Esta operación se realiza generalmente sobre un lote de componentes de seguridad, fabricados en serie. Después, el primer secreto se transmite al adquiriente del lote de componente de seguridad. A partir del conocimiento de este primer secreto, el adquiriente generalmente desea personalizar el primer secreto para cada componente introduciendo un secreto personalizado en cada componente. Esta etapa permite mejorar significativamente la seguridad del sistema, en concreto, generando un secreto conocido por solo el adquiriente. Pero esta etapa choca con el conocimiento del primer secreto, puesto que no es posible introducir un secreto personalizado sin el conocimiento del primer secreto. De ello se desprende que la introducción del secreto personalizado debe realizarse en un campo seguro con respecto, en concreto, al personal que puede acceder a los componentes en el transcurso de esta etapa. De este modo, los componentes se personalizan generalmente en unos locales seguros.

Para un sistema completo, por ejemplo, un sistema de billetes, que puede incluir un número importante de dispositivos que comprenden unos componentes de seguridad, repartidos sobre una zona geográfica importante, esta etapa de personalización resulta, por lo tanto, larga, costosa y poco flexible. Este inconveniente es particularmente sensible durante el despliegue de un sistema de este tipo.

Una solicitud de patente francesa (FR2873467A) describe un procedimiento de personalización de elementos electrónicos seguros sustituyendo un primer código secreto nativo por un segundo código secreto generado por un módulo de autentificación a partir, en concreto, del primer código secreto.

Una solicitud de patente internacional (WO2007/0521116A1), no publicada a fecha de presentación de la presente solicitud, describe, en concreto, un método de instalación y de inicialización de un elemento seguro.

La invención tiene como finalidad, en concreto, paliar los inconvenientes anteriormente citados. La invención tiene como objeto un procedimiento de personalización de un componente de seguridad que incluye:

- una etapa de inserción de un primer secreto K0 en dicho componente de seguridad, implementándose dicha etapa en un campo seguro bajo la responsabilidad del fabricante del componente de seguridad
- una etapa de generación de un secreto aplicativo K y una etapa de generación de un criptograma [K]K0 de personalización obtenido por cifrado del secreto aplicativo K por el primer secreto K0, implementándose dichas etapas en un campo seguro aplicativo bajo la responsabilidad del poseedor del componente de seguridad;
- una etapa de personalización del componente de seguridad por inserción en dicho componente de seguridad del criptograma [K]K0 de personalización, implementándose dicha etapa de personalización en un campo aplicativo.

El procedimiento incluye, además, una etapa en la que el primer secreto K0 se inserta en un componente de encriptado, implementándose dicha etapa en el campo seguro bajo la responsabilidad del fabricante del componente de seguridad. El componente de encriptado se utiliza para cifrar el secreto aplicativo K por el primer secreto K0 para generar el criptograma [K]K0 de personalización.

En un modo de realización, el número de utilizaciones posibles del componente de encriptado está limitado.

En otro modo de realización, un primer secreto diversificado $K0_{ND}$ se inserta en dicho componente de seguridad. El primer secreto diversificado $K0_{ND}$ se obtiene por cifrado de una información ND específica para el componente de seguridad con la ayuda de un secreto maestro KM. El secreto aplicativo K se inserta en la etapa de personalización del componente de seguridad por carga del criptograma $[K]K0_{ND}$ de personalización. La información ND puede ser el número de serie NS del componente de seguridad, o derivada del número de serie NS y/o de un contador N de utilizaciones irreversible.

Ventajosamente, la función de carga del secreto aplicativo K en el componente de seguridad de serie es irreversible.

La invención tiene, en concreto, como ventajas que permite que los datos sensibles cargados en un componente de seguridad permanezcan confidenciales en cualquier momento:

- Con respecto a cualquier persona exterior al sistema, incluso hostil, y que asiste a la operación de personalización;
- Con respecto a cualquier persona que opera la personalización, ya sea administrador o sencillo agente;
- Con respecto a cualquier persona interior al sistema aplicativo (diseñador, desarrollador...).

Además, la personalización de los componentes se efectúa sin necesidad de conexión externa. Los datos confidenciales pueden protegerse de la clonación, consistiendo la operación de clonación en volver a repetir los intercambios sobre otro componente del mismo tipo. Los datos confidenciales pueden protegerse de la repetición sobre el mismo componente.

Otras características y ventajas de la invención se mostrarán con la ayuda de la descripción que sigue hecha a la vista de los dibujos adjuntos que representan, la figura 1, un sinóptico del procedimiento según la invención de personalización de un componente de seguridad en medio no protegido.

La figura 1 ilustra por un sinóptico el procedimiento según la invención de personalización de un componente de seguridad en medio no protegido. El procedimiento según la invención tiene como objeto, en concreto, llevar a un componente de seguridad un secreto aplicativo K, que solo pueda fabricarse y utilizarse con la ayuda de un primer secreto K0 obtenido de un tercero de confianza. El tercero de confianza es, por ejemplo, el fabricante del componente él mismo. El componente de seguridad es, por ejemplo, de tipo módulo de acceso seguro (o según el acrónimo anglosajón SAM para Security Access Module).

De este modo, en una etapa 11, el fabricante inserta en el componente de seguridad el primer secreto K0. El primer secreto K0 puede insertarse físicamente en el circuito eléctrico del componente de seguridad o en el microprograma del componente de seguridad (o según la expresión anglosajona firmware). En el transcurso de esta etapa 11, el primer secreto K0 puede insertarse en un número importante de componentes de seguridad que forman uno o varios lotes, fabricados en serie.

En una etapa 12, el fabricante puede insertar el primer secreto K0, utilizado, en concreto, en la etapa 11, en un componente de encriptado, con el fin de disponer de un medio seguro que permita difundir para el adquiriente del componente de seguridad el primer secreto K0. El componente de encriptado es un medio adaptado para la generación del secreto aplicativo K con la ayuda de su secreto K0. Sin embargo, de manera ideal, el componente de encriptado no propone ningún medio de acceso al primer secreto K0 o limita el acceso a él haciendo la comprensión o el acceso físico difícil. Por ejemplo, el componente de encriptado adaptado para la generación del secreto aplicativo K puede ser un componente de seguridad de tipo módulo de acceso seguro, capaz de codificar cualquier valor por el primer secreto K0, no extraíble. De este modo, la inserción del primer secreto K0 en el componente de encriptado permite que el fabricante del componente no asegure ya necesariamente la retención de secretos que no sean el secreto K0. En efecto, el componente de encriptado se suministra a la salida de la etapa 12 al adquiriente de la serie de componentes de seguridad que contiene el primer secreto K0 a la salida de la etapa 11. El adquiriente podrá generar entonces un criptograma [K]K0 de personalización a partir del primer secreto K0 basado en un secreto K aplicativo.

Las operaciones llevadas a cabo dentro de las etapas 11 y 12 se realizan en un campo seguro 10 bajo la responsabilidad del fabricante del componente de seguridad. En efecto, el descubrimiento del primer secreto K0 por un atacante le permitiría encontrar el secreto aplicativo K vigilando el criptograma [K]K0. Esto es por lo que el secreto K0 no debe conocerse fuera del campo seguro 10 bajo la responsabilidad del fabricante. Además, el fabricante debe ser de confianza para garantizar la seguridad de los sistemas que implementan dichos componentes de seguridad. El componente de encriptado es sensible, pues posee el secreto K0 del fabricante, por una parte, y, por otra parte, puede experimentar un ataque que consiste en descubrir el secreto aplicativo K. En efecto, utilizar el componente de encriptado en desencriptado permitiría descubrir el secreto aplicativo K a partir del conocimiento del criptograma [K]K0, incluso sin conocer el primer secreto K0. Por esta razón, el componente de encriptado debe protegerse permitiendo la utilización de la función de encriptado y prohibiendo la utilización de la función de desencriptado. En un modo de realización, el ataque del componente de encriptado puede hacerse más difícil limitando el número de utilizaciones posibles del componente de encriptado. Esta limitación puede introducirse por el fabricante del componente de encriptado.

En una etapa 21, se genera el secreto aplicativo K. Después, en una etapa 22, se genera el criptograma [K]K0 de personalización. El criptograma de personalización corresponde al cifrado del secreto aplicativo K aplicativo generado en la etapa 21 por el primer secreto K0. El criptograma [K]K0 de personalización se obtiene utilizando el componente de encriptado para cifrar el secreto K con la ayuda del primer secreto K0. El criptograma [K]K0 de personalización no tiene necesariamente que tenerse secreto. El criptograma [K]K0 de personalización se difunde a continuación en una etapa 23 a otras personas, por ejemplo, a unas personas a cargo del despliegue del sistema.

Las operaciones llevadas a cabo dentro de las etapas 21, 22 se realizan en un campo seguro aplicativo 20 que compete al poseedor de las componentes de seguridad. Estas operaciones deben realizarse en un marco seguro:

por ejemplo, pueden llevarse a cabo en una fase de parametrización del sistema en unos locales seguros.

Después, en una etapa 31, el componente de seguridad se personaliza por inserción del criptograma [K]K0 de personalización generado en la etapa 22 y difundido en la etapa 23 fuera del campo seguro aplicativo 20. Entonces, el componente de seguridad comprende el criptograma [K]K0 de personalización, así como el primer secreto K0 insertado por el constructor en la etapa 11. De este modo, el componente de seguridad obtiene el conocimiento del secreto aplicativo K.

Las operaciones llevadas a cabo dentro de la etapa 31 se realizan en un campo no seguro aplicativo 30. Estas operaciones no deben realizarse necesariamente en un marco seguro: por ejemplo, pueden llevarse a cabo en una fase de instalación de un sistema en un lugar cualquiera sin vigilancia particular.

En un modo de realización, se realiza una función anticlonación en el componente de seguridad. El primer secreto K0 comprendido en los componentes de seguridad de uno o varios lotes fabricados en serie se diversifica para garantizar un nivel de seguridad adaptado para la necesidad del sistema. También, con el fin de introducir un primer secreto diferente para cada componente de seguridad comprendido en los diferentes lotes y para evitar la fabricación de tantos componentes de encriptado como de componentes de seguridad, es necesario generar unos primeros secretos obtenidos por diversificación de un secreto maestro KM. De este modo, el método de generación de los primeros secretos obtenidos por diversificación del primer secreto K0 debe ser determinista. Para ello, cada componente de seguridad de serie se fabrica con un primer secreto diversificado $K0_{ND}$ obtenido por el encriptado de una información ND (Número Diversificante) por el secreto KM, sea $K0_{ND}$ = [ND]KM. La información ND puede ser el número de serie NS del componente de seguridad. El primer secreto diversificado $K0_{ND}$ puede obtenerse con la ayuda de un solo componente de encriptado para el conjunto de los componentes de seguridades de los diferentes lotes. El secreto aplicativo K se inserta a continuación en la etapa 31 cargando el criptograma $[K]K0_{ND}$ de personalización. El criptograma $[K]K0_{ND}$ de personalización solo será utilizable para la carga del secreto aplicativo K sobre el componente de seguridad cuyo número diversificante sea igual a la información ND.

En un modo de realización, se realiza una función antirrepetición en el componente de seguridad. Por ejemplo, la orden de recarga del secreto aplicativo K en el componente de seguridad de serie es irreversible. Además, puede imponerse hacer depender la N+1ª carga del secreto K, anotado K_{N+1}, del secreto K_N, o del secreto K0 modificado por el valor N (por ejemplo, [N]K0), utilizando entonces el componente un contador irreversible de utilizaciones que contiene el valor N. Por lo tanto, el retorno al estado de fábrica del componente de seguridad es imposible.

Estos dos modos de realización, la diversificación del primer secreto K0 y la función antirrepetición, pueden combinarse, permitiendo, de este modo, hacer depender la carga del secreto K_{N+1} del secreto $[ND]K_N$, del secreto $[N]K0_{ND}$, o de cualquier otra combinación de ND, NS, N, K_N y $K0_{ND}$ que varían de un componente al otro o de una carga a la otra.

REIVINDICACIONES

1. Procedimiento de personalización de un componente de seguridad que incluye:

• una etapa (11) de inserción de un primer secreto K0 en dicho componente de seguridad, implementándose dicha etapa (11) en un campo seguro (10) bajo la responsabilidad del fabricante del componente de seguridad;
• una etapa (21) de generación de un secreto aplicativo K y una etapa (22) de generación de un criptograma [K]K0 de personalización obtenido por cifrado del secreto aplicativo K por el primer secreto K0, implementándose dichas etapas (21, 22) en un campo seguro aplicativo (20) bajo la responsabilidad del poseedor del componente de seguridad;
• una etapa (31) de personalización del componente de seguridad por inserción en dicho componente de seguridad del criptograma [K]K0 de personalización, implementándose dicha etapa (31) de personalización en un campo aplicativo (30).

caracterizado porque incluye, además, una etapa (12) en la que el primer secreto K0 se inserta en un componente de encriptado, implementándose dicha etapa (12) en el campo seguro (10) bajo la responsabilidad del fabricante del componente de seguridad, utilizándose dicho componente de encriptado para cifrar el secreto aplicativo K por el primer secreto K0 para generar (22) el criptograma [K]K0 de personalización.

2. Procedimiento según la reivindicación 1, **caracterizado porque** el número de utilizaciones posibles del componente de encriptado está limitado.

3. Procedimiento según una cualquiera de las reivindicaciones 1 y 2, **caracterizado porque** el primer secreto diversificado K0, insertado (11) en dicho componente de seguridad, es un primer secreto diversificado $K0_{ND}$ obtenido por cifrado de una información ND específica para el componente de seguridad con la ayuda de un secreto maestro KM, insertándose el secreto aplicativo K en la etapa (31) de personalización del componente de seguridad por carga del criptograma $[K]K0_{ND}$ de personalización.

4. Procedimiento según la reivindicación 3, **caracterizado porque** la información ND es el número de serie NS del componente de seguridad, o derivada del número de serie NS y/o de un contador N de utilizaciones irreversibles.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4 **caracterizado porque** la función de carga del secreto aplicativo K en el componente de seguridad de serie es irreversible.

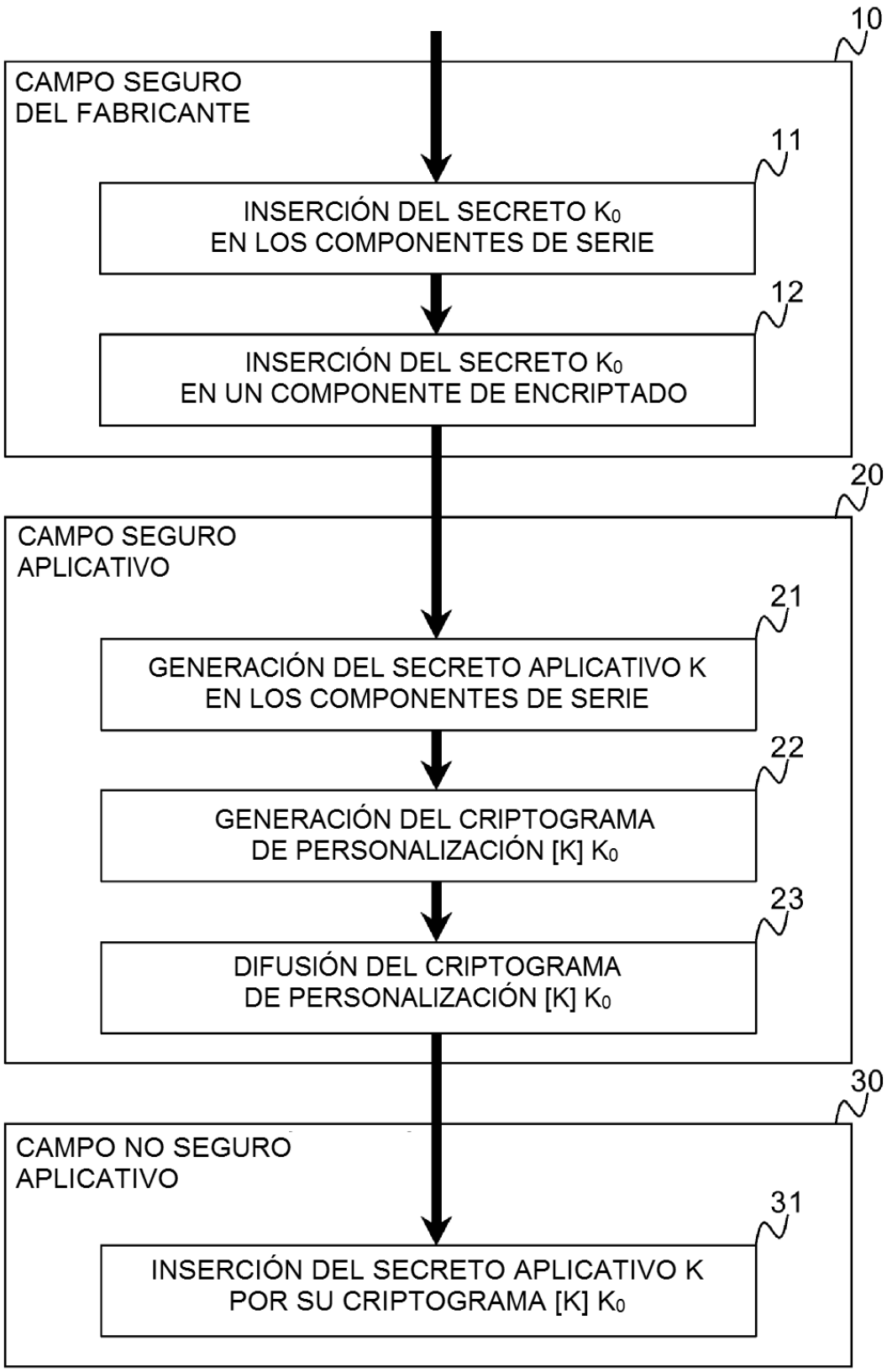
10
CAMPO SEGURO
DEL FABRICANTE
11
INSERCIÓN DEL SECRETO K0
EN LOS COMPONENTES DE SERIE
12
INSERCIÓN DEL SECRETO K0
EN UN COMPONENTE DE ENCRIPTADO
20
CAMPO SEGURO
APLICATIVO
21
GENERACIÓN DEL SECRETO APLICATIVO K
EN LOS COMPONENTES DE SERIE
22
GENERACIÓN DEL CRIPTOGRAMA
DE PERSONALIZACIÓN [K] K0
23
DIFUSIÓN DEL CRIPTOGRAMA
DE PERSONALIZACIÓN [K] K0
30
CAMPO NO SEGURO
APLICATIVO
31
INSERCIÓN DEL SECRETO APLICATIVO K
POR SU CRIPTOGRAMA [K] K0

FIG.1