(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 358 000**

(51) Int. Cl.:
G06F 21/02 (2006.01)
G06F 21/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08717183 .1**
(96) Fecha de presentación : **27.02.2008**
(97) Número de publicación de la solicitud: **2115656**
(97) Fecha de publicación de la solicitud: **11.11.2009**

(54) Título: **Procedimiento de modificación de secretos comprendidos en un módulo criptográfico, especialmente en medio no protegido.**

(30) Prioridad: **06.03.2007 FR 07 01625**

(45) Fecha de publicación de la mención BOPI:
04.05.2011

(45) Fecha de la publicación del folleto de la patente:
04.05.2011

(73) Titular/es: **THALES**
45, rue de Villiers
92200 Neuilly-sur-Seine, FR

(72) Inventor/es: **D'Athis, Thierry;**
Dailly, Philippe y
Ratier, Denis

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Procedimiento de modificación de secretos comprendidos en un módulo criptográfico, especialmente en medio no protegido.

La invención se refiere a un procedimiento de modificación de un conjunto de secretos comprendidos en un módulo criptográfico. En particular, la invención se aplica a la recarga en medio no protegido de claves de acceso comprendidas en un conjunto de tarjetas inteligentes.

En un sistema que comprende un conjunto de módulos criptográficos (por ejemplo tarjetas inteligentes que incluyen secretos criptográficos), la gestión de los secretos comprendidos en dichos módulos es una tarea compleja. En particular, la operación de puesta al día de los secretos, debe responder a un cierto número de exigencias de seguridad, Asimismo, es habitual que los secretos sean puestos a l día en medio seguro, es decir, generalmente en un local seguro, fuera del contexto de explotación de los módulos criptográficos. Cuando el número de módulos criptográficos es importante, esta operación de mantenimiento es pesada y costosa.

Además, con el fin de garantizar un nivel de seguridad correcto, los módulos criptográficos no permiten acceder en modo lectura y en modo escritura a los secretos. En caso de fallo del proceso de puesta al día de los secretos, por ejemplo tras una interrupción involuntaria del proceso, no es posible recuperar y acabar el proceso en el mismo lugar en que se ha producido tal fallo.

La invención tiene especialmente por objetivo paliar los inconvenientes citados anteriormente. Con este propósito, la invención tiene por objeto un procedimiento de modificación de secretos comprendidos en un módulo criptográfico. El módulo criptográfico garantiza, o bien que la carga de un secreto se ha completado o bien que no se ha producido. El módulo criptográfico permite la lectura de un número de versión por cada secreto. El módulo criptográfico incluye una información que indica un número de versión correspondiente al conjunto de los secretos. El procedimiento según la invención incluye especialmente una primera etapa a lo largo de la cual, si el número de versión del conjunto de los secretos es igual a un número de versión que requiere la carga de un conjunto de nuevos secretos, el número de versión del conjunto de los secretos del módulo criptográfico se vuelve igual a un número distintivo que permite determinar que el módulo criptográfico está en proceso de recarga. El procedimiento según la invención incluye una segunda etapa a lo largo de la cual, para cada secreto, si el número de versión de dicho secreto que corresponde a cargar, el nuevo secreto y su número de versión se cargan. El procedimiento según la invención incluye una tercera etapa a lo largo de la cual el número de versión del conjunto de los secretos del módulo criptográfico se vuelve igual al número de versión del conjunto de los nuevos secretos.

En una realización, el número de versión del conjunto de los secretos del módulo criptográfico en la tarjeta se graba en un fichero del módulo criptográfico de la tarjeta accesible por un secreto inmutable.

En otra realización, el número de versión del conjunto de los secretos del módulo criptográfico en la tarjeta se graba en forma de un secreto usado solamente para indicar la versión global de los secretos.

En otra realización, el número de versión del conjunto de los secretos del módulo criptográfico en la tarjeta se graba bajo la forma del último de los secretos a recargar en la segunda etapa.

En el curso de la etapa doce, la verificación del número de versión de cada secreto puede realizarse notablemente por una autentificación mutua de los diferentes secretos antes de encontrar el punto de interrupción.

La invención tiene especialmente como ventajas el hecho de que permite modificar un conjunto de secretos en un módulo criptográfico para de este modo garantizar la propia coherencia cuando la puesta al día no puede realizarse más que secreto por secreto. La invención permite también garantizar que después de la recarga de los secretos en el seno del módulo criptográfico, los datos ya presentes en el módulo criptográficos seguirán siendo accesibles y no corruptos. Asimismo, el procedimiento según la invención se puede interrumpir en cualquier instante sin que esto conlleve corrupción de los secretos comprendidos en el módulo criptográfico. Además, después de una o más interrupciones, voluntarias o accidentales, a lo largo de la aplicación de las etapas del procedimiento según la invención, el procedimiento se puede seguir aplicando desde la misma máquina o desde una máquina diferente capaz de proseguir con la aplicación de las etapas del procedimiento.

Otras características y ventajas aparecerán con la ayuda de la siguiente descripción respecto de los dibujos anexos que representan, en la figura 1, un cuadro sinóptico de las etapas del procedimiento según la invención de modificación de secretos comprendidos en un módulo criptográfico.

El procedimiento según la invención permite especialmente recuperar y acabar la modificación de un conjunto de secretos (datos sensibles dotados de sus claves de acceso), no pudiendo dichos secretos ser releídos, ni necesariamente reescritos.

En la realización del procedimiento según la invención, ilustrado por la figura 1, el módulo criptográfico que incluye los secretos, manipulado a lo largo de la aplicación de las etapas del procedimiento, tiene especialmente las siguientes características:

- garantía o bien de que la carga de un secreto se ha completado o bien de que no se ha producido (principio antidesgarro también designado por el término anglosajón de principio “anti-tear”);
- puesta al día simultánea del secreto y de su versión;
- posibilidad de leer un número de versión para cada secreto, no siendo por su parte dicho secreto accesible;

El módulo criptográfico incluye también una información que indica un número de versión que corresponde al conjunto de los secretos.

Tal módulo criptográfico puede ser por ejemplo una tarjeta inteligente, en particular una tarjeta “Mifare®DESfire”.

El procedimiento según la invención recibe en entrada un conjunto de nuevos secretos a cargar en vez y lugar de los secretos comprendidos en el módulo criptográfico. Al conjunto de nuevos secretos corresponde un número de versión correspondiente al conjunto de los nuevos secretos. Asimismo, al conjunto de los secretos comprendidos en el módulo criptográfico, corresponde un número de versión. A cada secreto comprendido en el módulo criptográfico corresponde un número de versión. A cada nuevo secreto a cargar corresponde un número de versión. a cada secreto corresponde por lo tanto un número de versión. Si los números de versión son idénticos entonces esto implica que los secretos son idénticos. Lo mismo ocurre para el número de versión del conjunto de los secretos.

El procedimiento según la invención incluye una primera etapa 1 a lo largo de la cual es módulo criptográfico se marca como que está en proceso de recarga de secretos. De este modo, a lo largo de la primera etapa 1, después de asegurarse, si fuese necesario, de que se ha solicitado la recarga de los secretos, se lee el número de versión del conjunto de los secretos del módulo criptográfico.

A continuación, el número de versión del conjunto de los secretos del módulo criptográfico se compara con el número de versión del conjunto de los secretos a cargar. Esta comparación determina si es necesario cargar los nuevos secretos (por ejemplo, el número de versión del conjunto de los secretos a cargar es superior al número de versión del conjunto de los secretos ya cargados). En su caso:

- el número de versión del conjunto de los secretos del módulo criptográfico se vuelve igual a un número distintivo que permite determinar que el módulo criptográfico está en proceso de recarga;
- a continuación, a lo largo de una segunda etapa 2 del procedimiento según la invención, para cada secreto, si el número de versión de dicho secreto es diferente del número de versión del nuevo secreto a cargar, se carga el nuevo secreto correspondiente así como su número de versión;
- y a continuación, a lo largo de una tercera etapa 3 del procedimiento según la invención, el número de versión del conjunto de los secretos del módulo criptográfico se vuelve igual al número de versión del conjunto de los nuevos secretos.

A lo largo de la primera etapa 1, si el número de versión del conjunto de los secretos del módulo criptográfico es igual al número distintivo que permite determinar que el módulo criptográfico está en proceso de recarga, esto significa que la operación de puesta al día no se ha podido llevar a cabo antes. En este caso:

- a lo largo de la etapa 2, para cada secreto, si el número de versión de dicho secreto es diferente del número de versión del nuevo secreto a cargar, se carga el nuevo secreto correspondiente así como su número de versión;
- y a continuación, a lo largo de una tercera etapa 3, el número de versión del conjunto de los secretos del módulo criptográfico se vuelve igual al número de versión del conjunto de los nuevos secretos.

Cualquier interrupción durante estas etapas se puede recuperar para de este modo proseguir con la recarga en el lugar interrumpido, e la misma máquina, o en otra máquina.

El número de versión del conjunto de los secretos del módulo criptográfico en la tarjeta se puede almacenar:

- bien en un fichero de la tarjeta accesible por un secreto inmutable;

- bien bajo la forma de la versión de un secreto particular, es decir:
    - bien un secreto que no sirve más que para dar la versión global de los secretos;
    - bien el último de los secretos a cargar en la etapa en que los secretos se cargan en un orden inmutable convenido.

En particular, el procedimiento según la invención se puede aplicar a un parque de tarjetas inteligentes que pueden tener números de versión de secretos diferentes. Este caso se presenta especialmente cuando el conjunto de las tarjetas inteligentes corresponde a un lote, y cuando los secretos son claves de acceso los datos. El procedimiento se puede aplicar a un parque de terminales sensibles cuyos secretos de comunicación se deben cambiar sobre el terreno. El procedimiento según la invención se puede aplicar asimismo a las bases de datos cuya administración no permite el cambio de los derechos de acceso en una sola transacción.

En una realización, la verificación del número de versión de cada secreto (en particular cuando ésta no está disponible o no es legible) se puede llevar a cabo mediante una autenticación mutua de los diferentes secretos hasta encontrar el punto de interrupción.

REIVINDICACIONES

1.- Procedimiento de modificación de secretos comprendidos en un módulo criptográfico, comprendiendo el módulo criptográfico:

- garantizar o bien que la carga de un secreto se ha completado o bien que no se ha producido.
- permitir la lectura de un número de versión para cada secreto;
- incluir una información que indica un número de versión correspondiente al conjunto de los secretos;

incluyendo el procedimiento:

- una primera etapa (1) a lo largo de la cual, si el número de versión del conjunto de los secretos es igual a un número de versión que requiere la carga de un conjunto de nuevos secretos, el número de versión del conjunto de los secretos del módulo criptográfico se hace igual a un número distintivo que permite determinar que el módulo criptográfico está en proceso de recarga;
- una segunda etapa (2) a lo largo de la cual, para cada secreto, si el número de versión de dicho secreto difiere del número de versión del nuevo secreto correspondiente a carga, se cargan el nuevo secreto y su número de versión.
- una tercera etapa (3) a lo largo de la cual el número de versión del conjunto de los secretos del módulo criptográfico se vuelve igual al número de versión del conjunto de los nuevos secretos.

2.- Procedimiento según la reivindicación 1, **caracterizado porque** siendo el módulo criptográfico una tarjeta inteligente, el número de versión del conjunto de los secretos del módulo criptográfico en la tarjeta se graba en un fichero del módulo criptográfico de la tarjeta accesible por un secreto inmutable.

3.- Procedimiento según la reivindicación 1, **caracterizado porque** siendo el módulo criptográfico una tarjeta inteligente, el número de versión del conjunto de los secretos del módulo criptográfico en la tarjeta se graba en forma de un secreto usado solamente para indicar la versión global de los secretos.

4.- Procedimiento según la reivindicación 1, **caracterizado porque** siendo el módulo criptográfico una tarjeta inteligente, el número de versión del conjunto de los secretos del módulo criptográfico en la tarjeta se graba bajo la forma del último de los secretos a recargar en la segunda etapa (2).

5.- Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** a lo largo de la segunda etapa (2), la verificación del número de versión de cada secreto se puede llevar a cabo mediante una autenticación mutua de los diferentes secretos hasta encontrar el punto de interrupción.

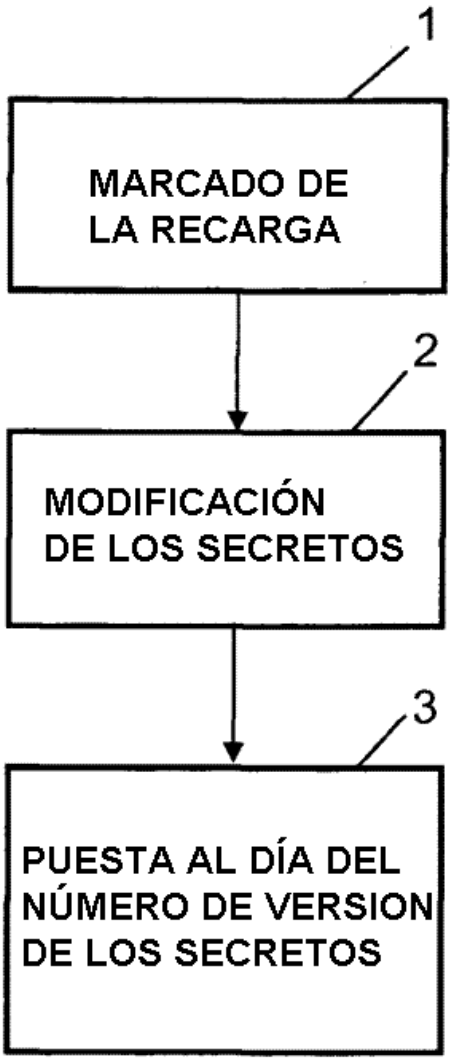
1
MARCADO DE LA RECARGA
2
MODIFICACIÓN DE LOS SECRETOS
3
PUESTA AL DÍA DEL NÚMERO DE VERSION DE LOS SECRETOS

FIG.1