(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 599 666**

(51) Int. CI.:

G06K 19/073 (2006.01)
G06K 19/07 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.05.2013 PCT/EP2013/060375**

(87) Fecha y número de publicación internacional: **28.11.2013 WO13174796**

(96) Fecha de presentación y número de la solicitud europea: **21.05.2013 E 13724257 (4)**

(97) Fecha y número de publicación de la concesión europea: **10.08.2016 EP 2852921**

(54) Título: **Procedimiento y tarjeta chip para transmitir información**

(30) Prioridad:

23.05.2012 FR 1254701

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.02.2017

(73) Titular/es:

MORPHO (100.0%)
11 Boulevard Galliéni
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

BERTHIER, MAËL;
GONCALVES, LOUIS-PHILIPPE;
LECOCQ, FRANÇOIS y
PEPIN, CYRILLE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento y tarjeta chip para transmitir información

La presente invención se refiere al campo de las tarjetas chip y, más en particular, a una tarjeta dotada de medios de transmisión de datos que utilizan canales de transmisión anejos.

Las tarjetas chip conocen un estado llamado de “final de vida útil” en el que, teóricamente, ya no es posible utilizar la tarjeta. La tarjeta se encuentra en este estado como respuesta a una anomalía o a un ataque. La tarjeta se bloquea y rehúsa todo funcionamiento, con el fin de conservar la integridad de los datos sensibles que contiene y de asegurarse de que no son sustraídos.

No obstante, sería ventajoso poder conocer el problema causante del paso de la tarjeta a este estado de final de vida útil.

Ahora bien, al estar bloqueada la tarjeta, no es posible comunicarse con ella. Además, pudiendo la causa del bloqueo de la tarjeta ser un ataque, es importante no comprometer los datos sensibles potencialmente contenidos en la tarjeta.

La invención se encamina a solucionar los anteriores problemas mediante un procedimiento de transmisión de datos por parte de una tarjeta chip en el final de su vida útil que utiliza canales de comunicación ocultos, diferentes de los canales de comunicación estándar de la tarjeta.

Los datos se transmiten mediante la modulación de una señal binaria que resulta de la modificación de un parámetro de soporte físico de la tarjeta.

De esta manera, la tarjeta dispone de un medio de emisión de una información de estado por un canal estrictamente monodireccional que no rebaja en lo más mínimo la seguridad de la tarjeta.

La invención se refiere a una tarjeta chip que comprende medios para transmitir datos que utilizan un canal de transmisión anejo, definido por el hecho de utilizar la modificación controlada de una característica de soporte físico de la tarjeta, detectable desde el exterior de la tarjeta.

De acuerdo con una forma de realización particular de la invención, esta está controlada por un primer sistema operativo dedicado al control de la tarjeta en su funcionamiento normal, e incluye un segundo sistema operativo dedicado al control de la transmisión de datos por canales anejos.

De acuerdo con una forma de realización particular de la invención, esta incluye un módulo de arranque que permite transferir el control hacia el segundo sistema operativo cuando la tarjeta está marcada como en situación de final de vida útil y, en caso contrario, hacia el primer sistema.

De acuerdo con una forma de realización particular de la invención, dicho segundo sistema incluye medios para emitir, a través del canal anejo, datos almacenados en un espacio de memoria compartido entre el primer y el segundo sistema.

De acuerdo con una forma de realización particular de la invención, el primer sistema comprende medios para, cuando la tarjeta pasa a final de su vida útil, copiar nuevamente datos destinados a ser transmitidos desde un espacio de memoria privado del primer sistema hacia el espacio de memoria compartido entre ambos sistemas.

De acuerdo con una forma de realización particular de la invención, el primer sistema comprende, además, medios de cifrado de los datos nuevamente copiados destinados a ser transmitidos.

De acuerdo con una forma de realización particular de la invención, el primer sistema comprende, además, medios para verificar la integridad de los datos nuevamente copiados destinados a ser transmitidos.

De acuerdo con una forma de realización particular de la invención, dicho canal anejo utiliza una codificación basada en la utilización de una misma instrucción, modificando la frecuencia de reloj de ejecución para modificar la cantidad de corriente consumida por la tarjeta en esta ejecución.

De acuerdo con una forma de realización particular de la invención, dicho canal anejo utiliza una codificación basada en la utilización de instrucciones del coprocesador criptográfico para modificar los campos electromagnéticos emitidos por este coprocesador que permiten la detección de su utilización.

Asimismo, la invención se refiere a un procedimiento de arranque de una tarjeta chip que incluye:

- una etapa de inicio de un módulo de arranque al dar tensión a la tarjeta;
- una etapa de prueba para determinar si la tarjeta está marcada como en situación de final de vida útil;

- una etapa de paso del control a un primer sistema si la tarjeta no está marcada como en situación de final de vida útil;

- una etapa de paso del control a un segundo sistema si la tarjeta está marcada como en situación de final de vida útil;

- una etapa de emisión de datos por parte de dicho segundo sistema que utiliza canales anejos, definidos por el hecho de utilizar la modificación controlada de una característica de soporte físico de la tarjeta, detectable desde el exterior de la tarjeta.

De acuerdo con una forma de realización particular de la invención, la etapa de emisión de datos por parte de dicho segundo sistema que utiliza canales anejos se repite regularmente mientras sea alimentada la tarjeta.

Las características de la invención antes mencionadas, así como otras, se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de un ejemplo de realización, descripción que se lleva a cabo en relación con los dibujos adjuntos, de los cuales:

la Fig. 1 ilustra la arquitectura de una tarjeta chip según la técnica anterior.

La Fig. 2 ilustra la arquitectura de una tarjeta chip según un ejemplo de realización de la invención.

La Fig. 3 ilustra el procedimiento de transmisión según un ejemplo de realización de la invención.

La Fig. 1 ilustra la arquitectura de una tarjeta chip 1.1. La tarjeta contiene un módulo de arranque 1.2 (*boot module*, en inglés). Este módulo se activa automáticamente al dar tensión a la tarjeta. Este módulo es el encargado de comprobar el estado de la tarjeta en el arranque. Típicamente, existen dos posibles estados para la tarjeta. Un primer estado es el estado de funcionamiento normal de la tarjeta. En este estado, el módulo de arranque pasa el control al sistema operativo 1.3 que moviliza la tarjeta. Este sistema operativo 1.3 utiliza al menos un espacio de almacenamiento de datos 1.5. Este administra igualmente un módulo de entradas - salidas 1.4 que permite los intercambios de datos con el entorno.

Asimismo, la tarjeta chip puede hallarse en un segundo estado, denominado estado de final de vida útil. El módulo de arranque, cuando reconoce que la tarjeta está en este estado de final de vida útil, no pasa el control al sistema operativo. Este interrumpe el funcionamiento de la tarjeta.

Una tarjeta operativa puede decidir pasar a final de su vida útil por un gran número de motivos. Puede ser la detección de un ataque o también la detección de una avería. El proceso de paso a final de vida útil comprende varias etapas. Se trata de proteger los datos sensibles contenidos en la tarjeta. Para conseguir esto, son borrados todos los datos borrables. Según el soporte físico utilizado, generalmente es posible bloquear el acceso a espacios de memoria bloqueando espacios de direcciones. Típicamente, se bloquean todos los espacios de direcciones que puedan serlo. Igualmente, se bloquean las entradas - salidas de la tarjeta. A continuación, la tarjeta es marcada como en situación de final de vida útil. Este marcado se realiza típicamente mediante el almacenamiento de un indicador (*flag*, en inglés) en memoria no volátil. Este indicador permanece accesible para el módulo de arranque. Por esta vía, el módulo de arranque tiene conocimiento del estado de la tarjeta.

La Fig. 2 ilustra la arquitectura de la tarjeta según un ejemplo de realización de la invención. Esta arquitectura rescata los elementos de la Fig. 1 referenciados con los mismos numerales. Contiene un segundo sistema 2.6, que tiene acceso a un espacio de almacenamiento compartido 2.7 entre el primer y el segundo sistema. El segundo sistema controla, además, un módulo de entradas - salidas 2.8. Este segundo sistema está dedicado a la transmisión de datos utilizando un canal de transmisión anejo de la tarjeta, administrado por el módulo de entradas - salidas 2.8. En la presente descripción, se define un canal de transmisión anejo como un canal de transmisión de datos que utiliza la modificación controlada de una característica física de la tarjeta, siendo esta modificación detectable y medible en intensidad desde el exterior de la tarjeta. Esta característica física, también llamada en adelante característica de soporte físico, puede ser la energía o la corriente eléctrica consumida por la propia tarjeta, la energía portada por ondas electromagnéticas o sonoras emitidas por la tarjeta o la energía térmica difundida por la tarjeta, o cualquier forma de energía que es emitida por la tarjeta. La información transmitida por este canal de transmisión anejo es codificada en forma de una modificación controlada, detectable y medible desde el exterior de la tarjeta, de una de estas características físicas.

Entonces, cuando la tarjeta pasa a final de vida útil, se copia información desde el espacio de almacenamiento 2.5 dedicado al primer sistema 2.3 hacia el espacio de almacenamiento compartido 2.7. Esta información es, típicamente, información de estado relacionada con la causa del paso a final de vida útil. Puede tratarse del módulo involucrado para la detección de una avería. Puede tratarse también del tipo de ataque detectado, si la causa del paso a final de vida útil es la detección de un ataque. Puede tratarse también de todo tipo de información de la que se desee disponer una vez la tarjeta en su final de vida útil. Esta nueva copia de información, así como su ocasional cifrado, es, típicamente, la única operación suplementaria relacionada con la invención que interviene en el paso de la tarjeta a su final de vida útil.

La Fig. 3 ilustra el procedimiento de arranque de la tarjeta según un ejemplo de realización de la invención.

En una primera etapa 3.1, la tarjeta arranca, típicamente como respuesta a la puesta en tensión de la misma. El control es encomendado automáticamente al módulo de arranque. Este, en una etapa 3.2, prueba si la tarjeta está en el final de su vida útil. Esta prueba se efectúa típicamente mediante la lectura del indicador previsto al efecto. Este indicador se encuentra ventajosamente en el espacio de memoria compartido de la tarjeta.

Si la tarjeta no está en el final de su vida útil, el control se pasa al primer sistema de la tarjeta, en la etapa 3.3. Entonces, la tarjeta funciona de manera totalmente normal. Esta utiliza el sistema normal de entradas - salidas para comunicarse con el exterior.

Si, por el contrario, la tarjeta está en el final de su vida útil, en lugar de interrumpirse, el módulo de arranque pasa el control al segundo sistema, en una etapa 3.4. El propósito de este segundo sistema es el de transmitir hacia el exterior la información de estado almacenada en el espacio de memoria compartido. Esta transmisión se efectúa en forma de una emisión de los datos a través de un canal de transmisión anejo.

Ventajosamente, la emisión de los datos prosigue de manera regular, mientras permanezca alimentada la tarjeta.

De acuerdo con una primera forma de realización de la invención, la característica de soporte físico utilizada por el canal anejo es el consumo de corriente de la tarjeta. En esta forma de realización, es posible modificar mediante soporte lógico la frecuencia de reloj de funcionamiento del procesador de la tarjeta. Se puede utilizar entonces una instrucción elegida del procesador que va a llamarse a diferentes frecuencias de reloj para codificar una información binaria. De acuerdo con el ejemplo de realización, se utiliza la instrucción 'NOP'. Esta instrucción no provoca cálculo alguno. No obstante, provoca un consumo de corriente dependiente de la frecuencia de reloj seleccionada. Es de señalar que el tiempo de ejecución de la instrucción depende asimismo de la frecuencia seleccionada, como también el tiempo del símbolo. Ventajosamente, un estado permite codificar un símbolo intermedio introducido entre dos símbolos binarios. Esto permite distinguir fácilmente dos símbolos sucesivos de igual valor.

De acuerdo con otra forma de realización, la característica de soporte físico utilizada es el funcionamiento del coprocesador criptográfico. Los símbolos son codificados en forma de instrucciones que utilizan, o no, el coprocesador criptográfico. Un registro de las emisiones electromagnéticas emitidas en la proximidad de este coprocesador permite recuperar una señal donde aparece la información de utilización de este coprocesador.

Cabe asimismo la posibilidad de utilizar la temperatura de la tarjeta, toda vez que ciertas instrucciones son conocidas por provocar un calentamiento del procesador, otras, menos. También se puede utilizar el sonido o los campos electromagnéticos.

El fundamento es que la información es codificada en forma de una evolución detectable y controlada de una característica de soporte físico de la tarjeta.

Habría sido posible utilizar las interfaces físicas de comunicación de la tarjeta, pero esto habría requerido implementar un controlador completo de comunicación en el seno del segundo sistema. Ahora bien, la solución adoptada puede ser implementada ventajosamente con la ayuda de solamente unas líneas de código. Basta con un lazo que lea los datos que han de emitirse y los codifique en forma de una serie de instrucciones que permitan modificar la característica física elegida. Al ser limitado el espacio de memoria en una tarjeta chip, esta sobriedad es ventajosa.

También hay que señalar que, pudiendo el final de vida útil estar provocado por una avería de la tarjeta, cuanto más limitados sean los recursos utilizados para implementar el segundo sistema, más aumentarán las posibilidades de que este esté operativo.

Por lo tanto, el interés de esta propuesta radica en la utilización de este protocolo de comunicación utilizando cualesquiera modificaciones del entorno medibles por la tarjeta. Ligado a la utilización de un protocolo de comunicación, está el hecho de que el código desarrollado con este motivo es compacto y se ejecuta al margen de cualquier código utilizado en el funcionamiento normal de la tarjeta. Ello hace de ésta una implementación protegida desde un punto de vista de la seguridad, ya que utiliza un código dedicado. No tiene que cambiarse ninguna de las seguridades ya presentes, y estas tienen que funcionar como de ordinario para hacer frente a cualquier ataque exterior.

El canal de comunicación así creado es estrictamente monodireccional. Esta característica es importante desde un punto de vista de la seguridad. A un atacante no le resulta posible utilizar este canal para escribir un dato en la tarjeta o para intentar provocar un comportamiento no deseado de la misma.

Solo pueden ser emitidos los datos previamente seleccionados y transferidos al espacio de memoria compartido. El segundo sistema no tiene acceso alguno al espacio de memoria administrado por el primer sistema, que potencialmente contiene datos sensibles.

La presente invención sirve principalmente para efectuar un diagnóstico que permite comprender cuáles son los

problemas que han impulsado a la tarjeta a pasar a final de vida útil. En este contexto, y a efectos de un ejemplo de utilización, es perfectamente posible cifrar los datos que han de enviarse al paso de la tarjeta a su final de vida útil. El mecanismo de cifrado y la clave utilizada han de elegirse de manera cuidadosa con el fin de conservar un buen nivel de seguridad. Ventajosamente, se utiliza un mecanismo de verificación de la integridad de los datos, típicamente una suma de comprobación de tipo CRC (*Cyclic Redundancy Check*, en inglés). Cuando la tarjeta está en el estado “en el final de su vida útil” y es alimentada, envía, mediante la utilización del mecanismo de la presente invención, simplemente los datos ya cifrados que están almacenados en memoria no volátil.

Más que una seguridad en el paso a final de vida útil de una tarjeta, este mecanismo también puede ser utilizado como parte integrante de un protocolo de comunicación y/o procedimiento de seguridad.

Por ejemplo, en la autenticación de una tarjeta, esta última puede enviar una información necesaria para el correcto desarrollo de la autenticación. Esto puede ser, por ejemplo, un evento o un número de serie. Se hace entonces más difícil, para un atacante, ver y comprender la información transmitida por esta vía. Habida cuenta de su función, los terminales pueden contar con medios para seguir el consumo de la tarjeta. Si esta última consume demasiado en un momento dado, esto puede considerarse un ataque y puede bloquear la tarjeta. Estos defectos son detectables, sobre todo, en la utilización de tarjetas falsificadas. De este modo, en un protocolo concertado entre el terminal y la tarjeta, se puede utilizar, en el contexto de una autenticación, un consumo superior para enviar un mensaje en un momento muy concreto, cuando, normalmente, tal consumo habría bloqueado la tarjeta. Se trata de un medio de ofrecer una mejor seguridad para la tarjeta y para el terminal que se comunicará con ella.

En esta forma de realización, el canal de datos anejo es utilizado por el primer sistema en el funcionamiento normal de la tarjeta. Este funcionamiento se lleva a cabo entonces paralelamente a un funcionamiento normal y a la utilización de los canales de transmisión normales de la tarjeta chip.

Según el canal anejo utilizado, el funcionamiento normal y la emisión de datos tienen que ser exclusivos en un momento dado para evitar que las perturbaciones de la característica de soporte físico elegida, provocadas por el funcionamiento normal de la tarjeta, lleguen a perturbar la emisión de los datos a través del canal anejo.

La invención descrita dentro del campo de las tarjetas chip concierne asimismo a todos los dispositivos de tratamiento de la información que utilizan chips del tipo tarjeta chip. Cabe citar, por ejemplo, dispositivos de memorias USB que contienen un chip de este tipo o también teléfonos que utilizan una tarjeta SIM (*Subscriber Information Module*, en inglés).

REIVINDICACIONES

1. Tarjeta chip, que comprende un primer sistema operativo dedicado al control de la tarjeta en su funcionamiento normal y un segundo sistema operativo dedicado al control de la transmisión de datos por al menos un canal anejo, caracterizada por que la tarjeta chip incluye, además:

- un módulo de arranque que permite transferir el control de la tarjeta chip hacia dicho segundo sistema operativo cuando la tarjeta está marcada como en situación en el estado "final de vida útil" y, en caso contrario, hacia dicho primer sistema operativo,

- utilizando dicho canal de transmisión anejo una modificación medible del entorno de dicha tarjeta para la transmisión de datos relativos a información de dicho estado "final de vida útil".

2. Tarjeta chip según la reivindicación 1, caracterizada por que dicho segundo sistema incluye medios para emitir, a través del canal anejo, dichos datos de estado "final de vida útil" almacenados en un espacio de memoria compartido entre el primer y el segundo sistema operativo.

3. Tarjeta chip según la reivindicación 2, caracterizada por que el primer sistema comprende medios para, cuando la tarjeta pasa al estado "final de vida útil", copiar nuevamente dichos datos de estado, destinados a ser transmitidos, desde un espacio de memoria privado del primer sistema operativo hacia el espacio de memoria compartido entre ambos sistemas operativos.

4. Tarjeta chip según la reivindicación 3, caracterizada por que el primer sistema comprende, además, medios de cifrado de dichos datos de estado nuevamente copiados destinados a ser transmitidos.

5. Tarjeta chip según la reivindicación 3 ó 4, caracterizada por que el primer sistema comprende, además, medios para verificar la integridad de dichos datos de estado nuevamente copiados destinados a ser transmitidos.

6. Tarjeta chip según una de las reivindicaciones 1 a 5, caracterizada por que dicho canal anejo utiliza la corriente consumida por dicha tarjeta para codificar dicha información de dicho estado "final de vida útil" en datos binarios.

7. Tarjeta chip según la reivindicación 6, caracterizada por que incluye medios para codificar dicha información de dicho estado "final de vida útil" en datos binarios, modificando la frecuencia de reloj de la ejecución de una misma instrucción, lo cual modifica la cantidad de corriente entonces consumida por dicha tarjeta en esta ejecución.

8. Tarjeta chip según una de las reivindicaciones 1 a 5, caracterizada por que dicho canal anejo utiliza los campos electromagnéticos emitidos por dicha tarjeta para codificar dicha información de dicho estado "final de vida útil" en datos binarios.

9. Tarjeta chip según la reivindicación 8, caracterizada por que incluye medios para codificar dicha información de dicho estado "final de vida útil" en datos binarios, utilizando instrucciones de un coprocesador criptográfico que incluye dicha tarjeta, lo cual modifica los campos electromagnéticos emitidos por este coprocesador.

10. Procedimiento de arranque de una tarjeta chip, caracterizado por que incluye:

- una etapa de prueba para determinar si la tarjeta está marcada como en situación en un estado "final de vida útil";

- una etapa de paso del control a un primer sistema operativo dedicado al control de la tarjeta en su funcionamiento normal, si la tarjeta no está marcada como en situación en un estado "final de vida útil" o, si la tarjeta está marcada como en situación en un estado "final de vida útil",

- una etapa de paso del control a un segundo sistema dedicado al control de la transmisión de datos relativos a información de dicho estado "final de vida útil" por al menos un canal anejo; utilizando dicho canal de transmisión anejo una modificación medible del entorno de dicha tarjeta para la transmisión de los datos relativos a información de dicho estado "final de vida útil".

11. Procedimiento según la reivindicación 10, caracterizado por que la etapa de paso del control a dicho segundo sistema operativo se repite regularmente mientras sea alimentada la tarjeta.

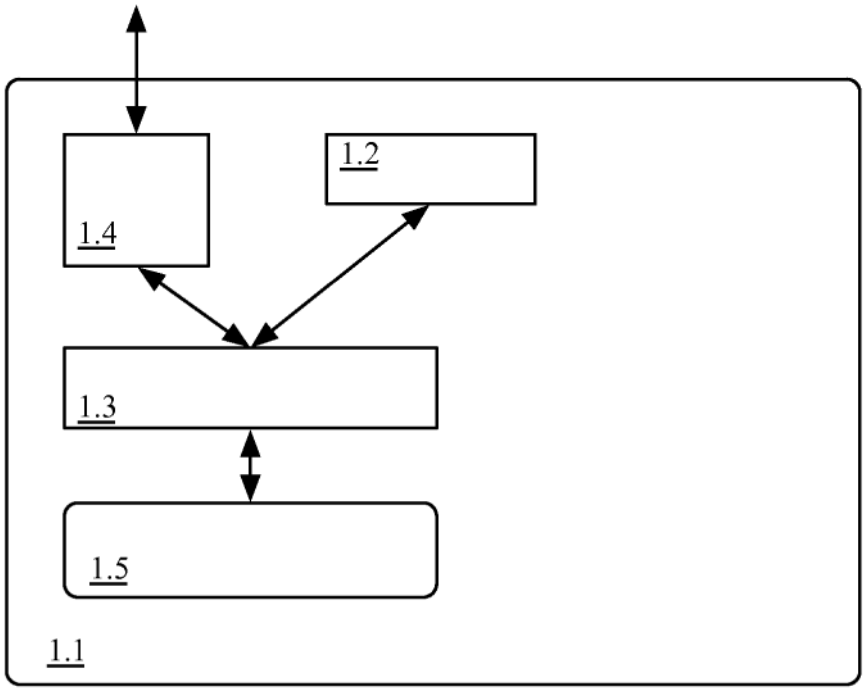

Fig. 1

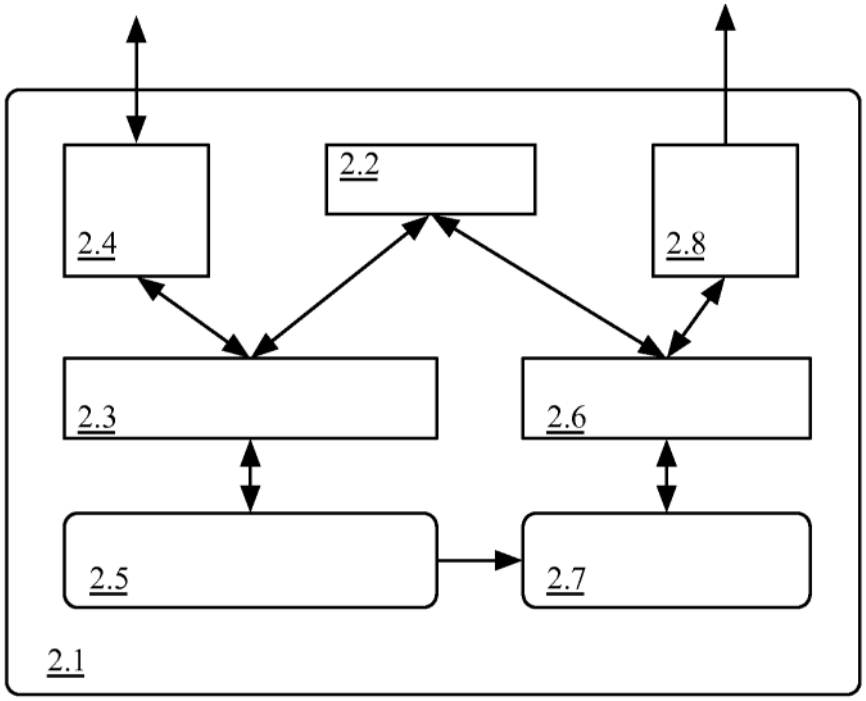

Fig. 2

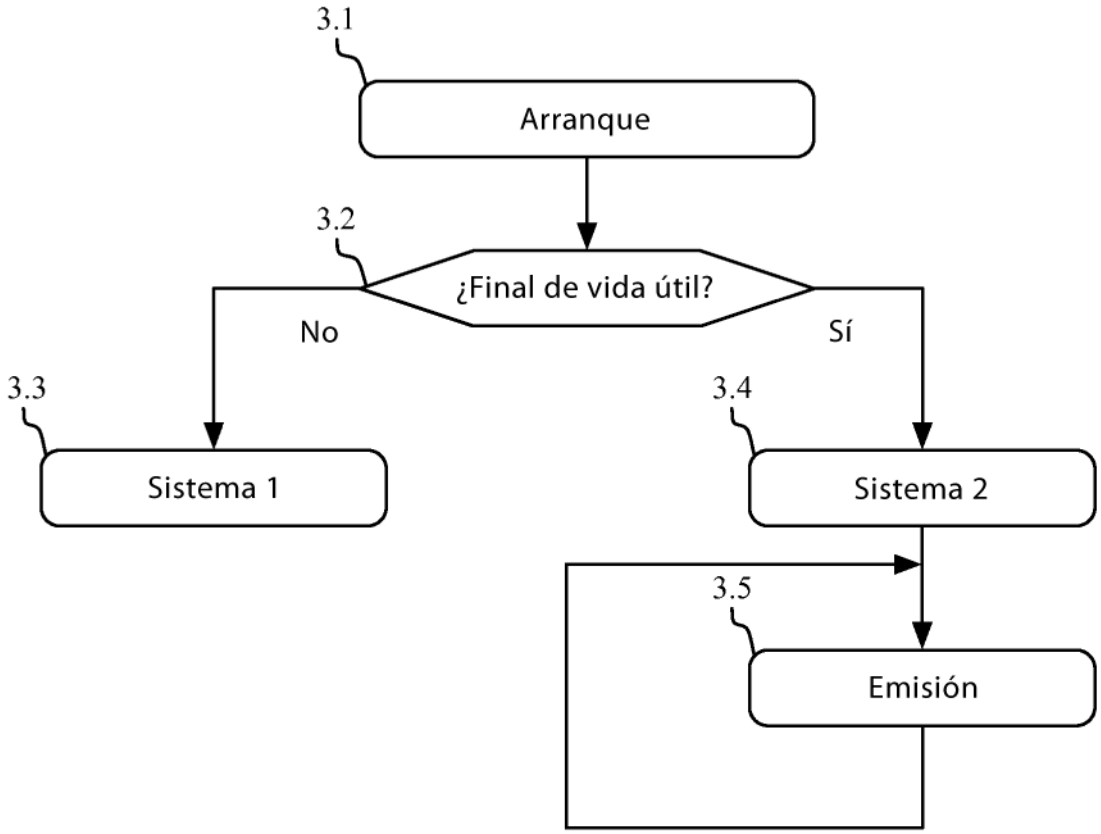
3.1
Arranque
3.2
¿Final de vida útil?
No
Sí
3.3
Sistema 1
3.4
Sistema 2
3.5
Emisión

Fig. 3