(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 755 990**

(51) Int. CI.:

G06F 21/78 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.07.2015 PCT/EP2015/065237**

(87) Fecha y número de publicación internacional: **18.02.2016 WO16023675**

(96) Fecha de presentación y número de la solicitud europea: **03.07.2015 E 15738870 (3)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 3180735**

(54) Título: **Método para gestionar varios perfiles en un elemento seguro**

(30) Prioridad:

12.08.2014 CN 201410393526

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2020

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

XIAO, YING;
DUPREZ, JÉROME y
DEHLINGER, FRANCK

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para gestionar varios perfiles en un elemento seguro

(Campo de la invención)

La presente invención se refiere a métodos para gestionar varios perfiles en un elemento seguro. En particular se refiere a métodos para gestionar varios perfiles en un elemento seguro en el que al menos un perfil está activo.

(Antecedentes de la invención)

Un elemento seguro es bien un componente físico resistente a la manipulación capaz de almacenar datos y prestar servicios de manera segura, bien un componente de *software* que proporciona un área de almacenamiento fiable y servicios fiables. En general, un elemento seguro tiene una cantidad limitada de memoria, un procesador con capacidades limitadas y no tiene batería. Por ejemplo, una UICC (Tarjeta de Circuito Integrado Universal) es un elemento seguro que incorpora aplicaciones SIM para fines de telecomunicaciones. Un elemento seguro se puede instalar, de forma fija o no, en un terminal, como por ejemplo un teléfono móvil. En algunos casos, los terminales están constituidos por máquinas que se comunican con otras máquinas para aplicaciones M2M (máquina a máquina).

Un elemento seguro puede tener el formato de una tarjeta inteligente, o puede tener cualquier otro formato, tal como por ejemplo, pero sin limitarse a, un chip empaquetado tal como se describe en el documento PCT/SE2008/050380, o cualquier otro formato. Una UICC se puede utilizar en terminales móviles en redes GSM, CDMA o UMTS, por ejemplo. La UICC garantiza la autentificación, integridad y seguridad en red de todo tipo de datos personales.

Ya se conoce el método consistente en soldar el elemento seguro en un dispositivo anfitrión, para que dependa de este dispositivo anfitrión. Esto se realiza en aplicaciones M2M (máquina a máquina). El mismo objetivo se alcanza cuando el dispositivo anfitrión contiene un chip (un elemento seguro) que contiene una aplicación de pago, aplicaciones SIM o USIM y archivos. El chip se suelda, por ejemplo, a la placa base de la máquina o dispositivo anfitrión y constituye un elemento seguro integrado (eSE, por sus siglas en inglés).

Un elemento seguro puede contener un perfil que puede incluir un conjunto de aplicaciones, un conjunto de datos personales y un conjunto de datos secretos. Los datos relacionados con un perfil se almacenan a través de una estructura de árbol lógico. Dicha estructura de árbol lógico comprende un archivo raíz y uno o varios directorios y archivos.

El perfil podría estar vinculado a un abono. Puede contener aplicaciones de acceso a la red (NAA, por sus siglas en inglés), aplicaciones de pago o aplicaciones de terceros que proporcionan seguridad para un servicio específico (por ejemplo, aplicaciones NFC).

Un elemento seguro físico puede emular varios elementos seguros virtuales, cada uno representado como un perfil. En tal caso, estos perfiles se denominan perfiles lógicos o perfiles virtuales. Un perfil emulado se llama en adelante perfil. Por lo general, cada perfil es un perfil basado en *software*.

La invención se refiere a una forma de gestionar varios perfiles que se ejecutan en un único elemento seguro.

En el estado actual de la técnica, solo se puede explorar la estructura de árbol lógico del perfil activo en un momento dado.

Es necesario permitir el acceso a la estructura de árbol lógico de un perfil diferente del perfil activo.

(Compendio de la invención)

Un objeto de la invención consiste en resolver el problema técnico arriba mencionado.

El objeto de la presente invención consiste en un elemento seguro que incluye un primer y un segundo perfiles que comprenden archivos organizados en estructuras de árbol lógico respectivas que comprenden archivos raíz respectivos. Estos archivos raíz tienen identificadores cuyos valores son diferentes de 0x3F00. El elemento seguro está configurado para permitir la exploración de la estructura de árbol lógico que comprende un archivo raíz objetivo en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar el archivo raíz objetivo.

Ventajosamente, el elemento seguro se puede configurar para seleccionar el archivo raíz del perfil actualmente activado en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual a 0x3F00.

Ventajosamente, el elemento seguro puede incluir una memoria no volátil que contiene un indicador que contiene el identificador del archivo raíz del perfil actualmente activado y el elemento seguro puede incluir un módulo de selección adaptado para seleccionar el archivo raíz del perfil actualmente activado utilizando el indicador al recibir un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual a 0x3F00.

Otro objeto de la invención consiste en un método para gestionar perfiles en un elemento seguro que incluye un primer y un segundo perfiles que comprenden archivos organizados en estructuras de árbol lógico respectivas que comprenden archivos raíz respectivos. Los archivos raíz tienen identificadores cuyos valores son diferentes de 0x3F00 y el método comprende la etapa consistente en habilitar la exploración de la estructura de árbol lógico que comprende un archivo raíz objetivo en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar dicho archivo raíz objetivo.

Ventajosamente, el método puede comprender la etapa consistente en seleccionar el archivo raíz del perfil actualmente activado en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual a 0x3F00.

Otro objeto de la invención consiste en un dispositivo anfitrión que comprende un elemento seguro de acuerdo con la invención, en el que el elemento seguro es una UICC o una UICC integrada (eUICC).

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención surgirán más claramente de una lectura de la siguiente descripción de una serie de realizaciones preferidas de la invención con referencia a los dibujos adjuntos correspondientes, en los que:

- la Figura 1 es un ejemplo de un dispositivo anfitrión que incluye un elemento seguro de acuerdo con la invención,

- la Figura 2 muestra un ejemplo de tipo de archivo para estructuras de árbol lógico en un elemento seguro de acuerdo con la invención, y

- la Figura 3 muestra un ejemplo de identificador de archivo para estructuras de árbol lógico integradas en un elemento seguro de acuerdo con la invención.

(Descripción detallada de las realizaciones preferidas)

La invención se puede aplicar a cualquier tipo de elemento seguro destinado a contener varios perfiles. El elemento seguro se puede acoplar a cualquier tipo de dispositivo anfitrión capaz de establecer una sesión de comunicación con el elemento seguro. Por ejemplo, el dispositivo anfitrión puede ser un teléfono móvil, una tableta, un vehículo, un medidor, una máquina expendedora, un televisor o un ordenador.

En esta memoria descriptiva, la notación "0x" se refiere a un número expresado en hexadecimal. Por ejemplo, 0x1234 es igual a 4660 en decimal.

En esta memoria descriptiva, el comando de selección de archivo se refiere al comando SELECCIONAR ARCHIVO que permite seleccionar un archivo tal como se define en la norma ISO/IEC 7816-4, GSM 11.11 v8.3.0 o ETSI TS 102221 v11.0.0. Este comando permite seleccionar bien un archivo raíz, bien un directorio o un archivo. Tal como se define en la norma ISO/IEC 7816-4, el valor 0x3F00 está reservado para el archivo raíz (también llamado archivo maestro).

Una estructura de árbol lógico es un conjunto de directorios y archivos que están estructurados como un árbol. En esta memoria descriptiva, una estructura de árbol lógico es una estructura de árbol jerárquica que se puede considerar como un sistema de archivos autónomo.

De acuerdo con la invención, a cada perfil integrado en el elemento seguro se le asigna un archivo raíz que tiene un valor de identificador diferente de 0x3F00.

Los identificadores de los archivos raíz son únicos para cada perfil. Estos archivos raíz pueden tener un identificador igual a cualquier valor diferente de 0x3F00. Cada archivo raíz tiene su propio valor de identificador que se puede determinar sin ambigüedades. Preferiblemente, los valores de identificador de los archivos raíz se establecen de modo que no haya colisión, incluso si se utiliza el mecanismo de Identificador de Archivo Corto (SFI, por sus siglas en inglés).

La **Figura 1** muestra un dispositivo anfitrión HO que comprende un elemento seguro SC de acuerdo con la invención.

En este ejemplo, el dispositivo anfitrión HO es un teléfono móvil que tiene una interfaz de comunicación de *hardware* para comunicarse con el elemento seguro.

El elemento seguro SC es una UICC que comprende una interfaz de comunicación IN, un módulo de procesamiento MP, una memoria volátil ME2 y una memoria no volátil ME1. La memoria no volátil ME1 comprende un sistema operativo OS y los perfiles PR1 y PR2.

La memoria no volátil ME1 comprende un módulo de guía M2 configurado para permitir la exploración de la estructura de árbol lógico que comprende el archivo raíz establecido explícitamente como objetivo por un comando Seleccionar archivo recibido. Más concretamente, en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo raíz específico, el módulo guía M2 se configura para seleccionar el archivo raíz específico.

La memoria no volátil ME1 comprende el indicador FL que almacena un valor que refleja el perfil actualmente activo. La memoria no volátil ME1 comprende un módulo de selección M1 configurado para seleccionar el archivo raíz del perfil actualmente activo en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador igual a 0x3F00. Cabe señalar que el elemento seguro SC no comprende ningún archivo raíz con el valor de identificador 0x3F00.

En otra realización, el sistema operativo OS se puede configurar para gestionar un indicador que apunta al archivo raíz del perfil actualmente activo y se puede diseñar para seleccionar este archivo raíz en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador igual a 0x3F00. En tal caso, el indicador FL y el módulo de selección M1 ya no son necesarios.

La **Figura 2** muestra un ejemplo de dos estructuras de árbol lógico correspondientes a dos perfiles PR1 y PR2 en un elemento seguro SC de acuerdo con la invención.

El primer perfil PR1 comprende una estructura de árbol lógico que incluye un archivo raíz RF1 que comprende dos directorios D1 y D2. El directorio D1 comprende un archivo F1 y el directorio D2 comprende dos archivos F2 y F3.

El segundo perfil PR2 comprende una estructura de árbol lógico que incluye un archivo raíz RF2 que comprende dos directorios D3 y D4. El directorio D3 comprende un archivo F4 y el directorio D4 comprende un archivo F6. El archivo raíz RF2 se considera como un directorio y comprende un archivo F5.

La **Figura 3** muestra un ejemplo de identificadores utilizados para las dos estructuras de árbol lógico de la Figura 2.

El archivo raíz RF1 tiene un identificador igual a 0x3F01. El directorio D1 tiene un identificador igual a 0xDF01. El directorio D2 tiene un identificador igual a 0xDF02. El archivo F1 tiene un identificador igual a 0xEF01. El archivo F2 tiene un identificador igual a 0xEF02. El archivo F3 tiene un identificador igual a 0xEF03.

El archivo raíz RF2 tiene un identificador igual a 0x3F02. El directorio D3 tiene un identificador igual a 0xDF03. El directorio D4 tiene un identificador igual a 0xDF04. El archivo F4 tiene un identificador igual a 0xEF04. El archivo F5 tiene un identificador igual a 0xEF05. El archivo F6 tiene un identificador igual a 0xEF06.

A continuación se describe un ejemplo de un método de acuerdo con la invención a partir de los perfiles descritos en la Figura 3. Se supone que el perfil PR1 se ha activado previamente. Por defecto, la estructura de árbol lógico del perfil PR1 es la actual.

Cuando el dispositivo anfitrión necesita acceder a la estructura de árbol lógico del perfil PR2, puede enviar un comando de selección de archivo dirigido al identificador 0x3F02.

Al recibir este comando de selección de archivo, el elemento seguro permite explorar la estructura de árbol del perfil PR2 y selecciona el archivo raíz RF2. Por lo tanto, el archivo raíz RF2 es ahora el archivo actual en el elemento seguro, mientras que el perfil PR1 sigue siendo el perfil actualmente activado.

En otra etapa, cuando el dispositivo anfitrión necesita acceder a la estructura de árbol lógico del perfil PR1, puede enviar un comando de selección de archivo dirigido al identificador 0x3F00 o 0x3F01.

De acuerdo con la invención, el elemento seguro interpreta el identificador con el valor 0x3F01 como una selección del archivo raíz del perfil PR1. Al recibir el comando de selección de archivo, el elemento seguro permite explorar la estructura de árbol del perfil PR1 y selecciona el archivo raíz RF1. Por lo tanto, el archivo raíz RF1 es ahora el archivo actual en el elemento seguro.

Según una realización de la invención, el elemento seguro interpreta el identificador con el valor 0x3F00 como el archivo raíz que pertenece a la estructura de árbol lógico del perfil actualmente activo. Como el perfil activo sigue siendo el perfil PR1, se selecciona el archivo raíz 0x3F01 y se puede acceder a su estructura de árbol lógico a través del mecanismo de exploración habitual. Por lo tanto, el archivo raíz RF1 ahora es el archivo actual en el elemento seguro.

Ventajosamente, cuando el mensaje de respuesta correspondiente al comando de selección de archivo está destinado a enviar de vuelta el identificador del archivo seleccionado, el elemento seguro envía un mensaje de respuesta que comprende el valor de identificador 0x3F00 incluso si el archivo realmente seleccionado tiene el valor de identificador 0x3F01.

Gracias a la invención, el dispositivo que envía el comando de selección de archivo puede acceder fácilmente a archivos de cualquier perfil objetivo.

Gracias a la invención, el elemento seguro es compatible con los dispositivos anfitriones que seleccionan el archivo raíz del perfil actual de forma habitual (es decir, "seleccionar 0x3F00").

Una ventaja de la invención consiste en que permite el acceso a la estructura de árbol lógico de un perfil diferente del perfil activo sin cambiar el perfil actualmente activo.

Debe entenderse, dentro del alcance de la invención, que las realizaciones arriba descritas se proporcionan como ejemplos no limitativos. En particular, el elemento seguro puede comprender cualquier número de perfiles y estos perfiles pueden estar relacionados con diferentes tipos de abono y diferentes dominios, como pago, telecomunicaciones, acceso de transporte, identidad, medición, acceso de video o acceso a servicios en la nube, por ejemplo.

Cabe señalar que los comandos de selección de archivo pueden ser enviados por una máquina remota distinta del dispositivo anfitrión que aloja el elemento seguro.

La arquitectura del dispositivo anfitrión y la arquitectura del elemento seguro que se muestran en la Figura 1 se proporcionan solo como ejemplos. Estas arquitecturas pueden ser diferentes. Por ejemplo, el módulo de selección M1 y el módulo de guía M2 pueden fusionarse como un solo módulo.

La invención es aplicable a cualquier tipo de elemento seguro capaz de recibir un comando de selección de archivo. En particular, la invención es aplicable a elementos seguros de tipo UICC y de tipo UICC integrada.

REIVINDICACIONES

1. Un elemento seguro (SC) que incluye un primer y un segundo perfiles (PR1, PR2) que comprenden archivos organizados en las respectivas primera y segunda estructuras de árbol lógico,

caracterizado por que dicha primera estructura de árbol lógico incluye un primer archivo raíz (RF1) y dicha segunda estructura de árbol lógico incluye un segundo archivo raíz (RF2), por que dichos archivos raíz (RF1, RF2) tienen identificadores cuyos valores son diferentes de 0x3F00 y por que dicho elemento seguro (SC) está configurado para permitir la exploración de la estructura de árbol lógico que comprende un archivo raíz objetivo en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar dicho archivo raíz objetivo.

2. Un elemento seguro (SC) según la reivindicación 1, estando configurado dicho elemento seguro (SC) para seleccionar el archivo raíz del perfil actualmente activado en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual a 0x3F00.

3. Un elemento seguro (SC) según la reivindicación 2, incluyendo dicho elemento seguro (SC) una memoria no volátil (ME1) que contiene un indicador (FL) que contiene el identificador del archivo raíz del perfil actualmente activado, e incluyendo dicho elemento seguro (SC) un módulo de selección (M1) adaptado para seleccionar el archivo raíz del perfil actualmente activado mediante el uso del indicador (FL) al recibir un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual a 0x3F00.

4. Un elemento seguro (SC) según la reivindicación 2, incluyendo dicho elemento seguro (SC) un sistema operativo configurado para gestionar un indicador que apunta al archivo raíz del perfil actualmente activo y para seleccionar el archivo raíz del perfil actualmente activo en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador igual a 0x3F00.

5. Un elemento seguro (SC) según la reivindicación 2, estando configurado dicho elemento seguro (SC) para enviar un mensaje de respuesta que comprende un identificador cuyo valor es igual a 0x3F00 en respuesta a dicho comando de selección de archivo.

6. Un elemento seguro (SC) según la reivindicación 1, en donde, estando activado dicho primer perfil (PR1), dicho elemento seguro (SC) está configurado para seleccionar el segundo archivo raíz (RF2) en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual al valor de identificador del segundo archivo raíz (RF2), y para mantener dicho primer perfil (PR1) activado.

7. Un método para gestionar perfiles en un elemento seguro (SC), incluyendo dicho elemento seguro (SC) un primer y un segundo perfiles (PR1, PR2) que comprenden archivos organizados en las respectivas primera y segunda estructuras de árbol lógico,

caracterizado por que dicha primera estructura de árbol lógico incluye un primer archivo raíz (RF1) y dicha segunda estructura de árbol lógico incluye un segundo archivo raíz (RF2), por que dichos archivos raíz (RF1, RF2) tienen identificadores cuyos valores son diferentes de 0x3F00 y por que dicho método comprende la etapa consistente en permitir la exploración de la estructura de árbol lógico que comprende un archivo raíz objetivo en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar dicho archivo raíz objetivo.

8. Un método según la reivindicación 7, comprendiendo dicho método la etapa consistente en seleccionar el archivo raíz del perfil actualmente activado en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual a 0x3F00.

9. Un método según la reivindicación 8, en el que dicho elemento seguro (SC) envía un mensaje de respuesta que comprende un identificador cuyo valor es igual a 0x3F00 en respuesta a dicho comando de selección de archivo.

10. Un método según la reivindicación 7, en el que, estando activado dicho primer perfil (PR1), dicho elemento seguro (SC) selecciona el segundo archivo raíz (RF2) en respuesta a la recepción de un comando Seleccionar archivo destinado a seleccionar un archivo que tenga un identificador cuyo valor sea igual al valor de identificador del segundo archivo raíz (RF2), y mantiene dicho primer perfil (PR1) activado.

11. Un dispositivo anfitrión (HO) que comprende un elemento seguro (SC) según la reivindicación 1, en el que el elemento seguro (SC) es una UICC o una eUICC.

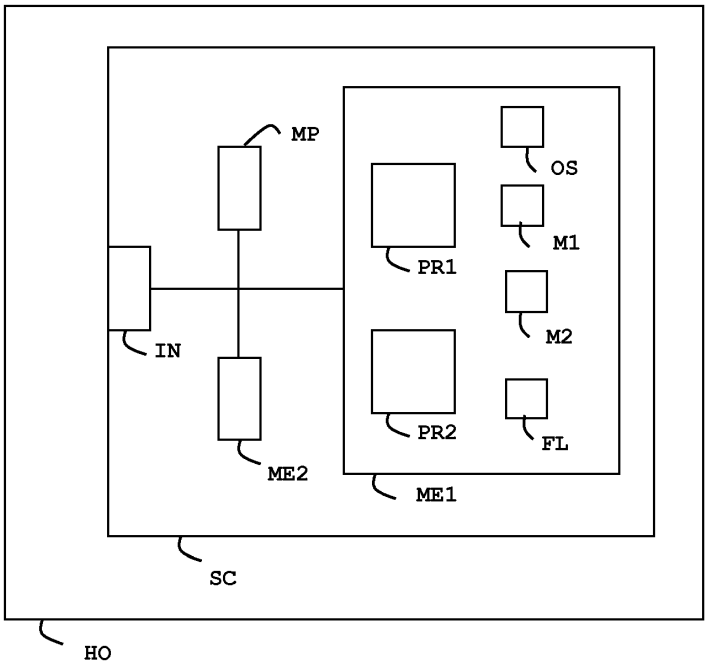

FIG. 1

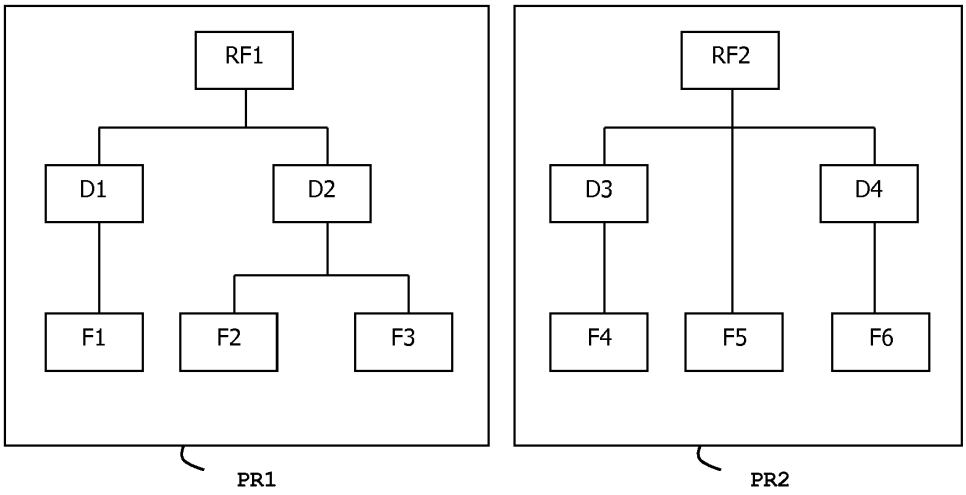
RF1
D1
D2
F1
F2
F3
PR1
RF2
D3
D4
F4
F5
F6
PR2

FIG. 2

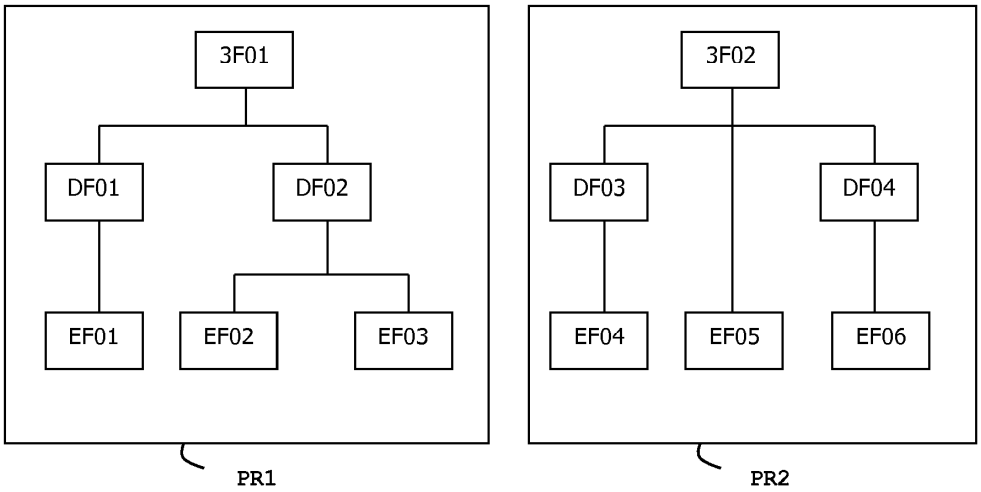
3F01
DF01
DF02
EF01
EF02
EF03
PR1
3F02
DF03
DF04
EF04
EF05
EF06
PR2

FIG. 3