(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 449 073**

(51) Int. CI.:

H04M 1/725 (2006.01)
H04W 88/02 (2009.01)
G06F 9/44 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.10.2006 E 06820297 (7)**

(97) Fecha y número de publicación de la concesión europea: **25.12.2013 EP 1946206**

(54) Título: **Procedimiento y sistema de gestión de las aplicaciones de un terminal móvil**

(30) Prioridad:

17.10.2005 FR 0510575

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2014

(73) Titular/es:

ORANGE (50.0%)
78, rue Olivier de Serres
75015 Paris, FR y
NXP B.V. (50.0%)

(72) Inventor/es:

KERDRAON, ALAN;
MOREL, THIERRY;
BRIOT, OLIVIER;
LEGROS, JÉRÔME y
MEYN, HAUKE

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Procedimiento y sistema de gestión de las aplicaciones de un terminal móvil.

Campo técnico de la invención

La invención se refiere al campo de las telecomunicaciones móviles, y más particularmente al de la gestión de las aplicaciones de un terminal móvil.

Antecedentes de la invención

En la actualidad, un usuario de un terminal móvil del tipo teléfono móvil o teléfono inteligente “smart phone” se enfrenta a una oferta de servicios cada vez más abundante. Más allá de los servicios clásicos de telefonía, se le propone al usuario un conjunto de servicios diversos y variados, como servicios de mensajerías, de flujo continuo “streaming” de audio y vídeo, de juegos, de descarga de contenido, de agenda, etcétera. Estos servicios son accesibles o bien de manera local en el terminal móvil, o bien por medio de una red móvil (GSM, GPRS, UMTS, etcétera), o bien incluso en situación de proximidad, por ejemplo por medio de los protocolos de intercambio tales como el IrDA, Bluetooth o el RFID.

Estos servicios se basan en aplicaciones que se almacenan o bien directamente en el terminal móvil o bien en las tarjetas chip o tarjetas inteligentes “SmartCard”. Se observará que un servicio puede hacer referencia a una o varias aplicaciones.

Por ejemplo, en el sistema Java, cuando una aplicación se encuentra en el terminal móvil, se corresponde con una miniaplicación denominada MIDlet (*Mobile Information Device Profile Applet*), es decir, una aplicación Java ejecutable en un móvil Java. Así, la parte de presentación (por ejemplo, MIDlet Java) que gestiona la interfaz hombre máquina (IHM) de la aplicación es propia del terminal móvil en el cual se ejecuta. La misma se hace cargo de la interfaz gráfica de la aplicación así como de la gestión del acceso a ciertos recursos del terminal móvil o de la red (por ejemplo establecimiento de una comunicación GSM, conexión a un servidor WAP, envío de un SMS, etcétera). Se observará que una MIDlet es en general una miniaplicación específica que no facilita la integración de una aplicación nueva en el terminal móvil.

Por otra parte, cuando una aplicación se encuentra en una tarjeta inteligente (SmartCard) de tipo tarjeta chip, se corresponde con una *Cardlet* (JavaCard Applet). En este caso, la parte de negocio (por ejemplo, Cardlet Java) que gestiona los datos de la aplicación se puede almacenar o bien en una tarjeta SIM del terminal móvil o bien en un componente específico como, por ejemplo, un SMART MX.

Es importante señalar que el despliegue y la gestión de estas aplicaciones, también denominadas “tarjetas”, no están normalizados, de modo que cada proveedor de tarjetas propone su propia solución en términos particularmente de gestión. Así, la multiplicación de las tarjetas o aplicaciones hace que aumente la complejidad de gestión de estas aplicaciones por parte del usuario.

El documento US 2005/0006461 describe un terminal móvil que memoriza las transacciones de una aplicación. Los documentos FR 2 857 193, WO 98/32089 y WO 2005/020604 describen comunicaciones entre una tarjeta que memoriza una aplicación y un terminal.

Objeto y resumen de la invención

La invención se refiere a un sistema de gestión según la reivindicación 1.

La invención se refiere asimismo a una tarjeta según la reivindicación 3.

Breve descripción de los dibujos

Otras particularidades y ventajas de la invención se pondrán de manifiesto al leer la descripción siguiente realizada a título indicativo aunque no limitativo, en referencia a los dibujos adjuntos, en los cuales:

- la figura 1 es una vista esquemática de un sistema de gestión de un terminal móvil que comprende una pluralidad de aplicaciones según la invención;
- las figuras 2 y 3 son unos ejemplos esquemáticos que ilustran unas vistas detalladas de la figura 1;
- la figura 4 es una vista esquemática de un modo de realización particular del sistema de gestión de la figura 3; y
- las figuras 5 a 13 son unos esquemas dinámicos que describen el funcionamiento entre los diferentes

elementos del sistema de gestión del terminal móvil según la invención.

Descripción detallada de modos de realización

La figura 1 ilustra un ejemplo de un sistema de gestión 1 de un conjunto de aplicaciones 3 almacenado en un terminal móvil según la invención. Por conjunto de aplicaciones, se entiende una o varias aplicaciones. Este sistema comprende un gestor de aplicaciones 5 (*Applications Handler*) destinado a gestionar por lo menos una aplicación 3. El gestor de aplicaciones 5 comprende un medio de acceso 7 al conjunto de aplicaciones 3, que permite que dicha por lo menos una aplicación 3 acceda a por lo menos una función determinada. Así, este medio de acceso 7 es un acceso común a un conjunto de aplicaciones 3 instaladas en el terminal móvil, que permite normalizar la gestión de estas aplicaciones 3 y facilitar la integración de cualquier aplicación nueva. A título de ejemplo, el medio de acceso 7 puede corresponder a unas aplicaciones “JAVA” de tipo “javacard”.

Además, la figura 2 muestra que el gestor de aplicaciones 5 comprende un medio de almacenamiento 9 al que se puede denominar directorio de aplicaciones (*Repository*) así como eventualmente un registro de transacciones 11 (*Transaction Log*) y un módulo de seguridad 13.

Así, el medio de almacenamiento 9 permite la grabación de las informaciones relativas a cualquier aplicación 3 ya instalada en el terminal móvil o a cualquier aplicación nueva que se vaya a integrar en el terminal móvil. El medio de almacenamiento 9 puede comprender, por ejemplo, una lista de las aplicaciones 3 instaladas en el terminal móvil así como de los parámetros asociados a cada una de estas aplicaciones 3. Se observará que una aplicación puede ser gestionada por el gestor de aplicaciones 5 cuando la misma está grabada en el medio de almacenamiento 9.

El registro de transacciones 11 permite la grabación de las informaciones relativas a las transacciones realizadas por el usuario a partir del terminal móvil. Estas informaciones pueden comprender las fechas de inicio y final de la transacción así como el resultado de la transacción.

Asimismo, el módulo de seguridad 13 permite la administración de datos de seguridad que comprenden, por ejemplo, códigos y claves de seguridad relativos a cualquier aplicación 3.

La figura 3 ilustra un ejemplo más detallado de la figura 1, que muestra que el sistema de gestión 1 comprende un medio de gestión centralizada 15 (*Applications Manager*) conectado al gestor de aplicaciones 5. Este medio de gestión centralizada 15 permite la generación de una vista unificada de dicha por lo menos una aplicación 3 gestionada por el gestor de aplicaciones 5.

Más particularmente, el medio de gestión centralizada 15 comprende una interfaz gráfica de usuario 17 (GUI *Graphique User Interface*) y un conector 19. Este último, el cual puede adoptar la forma de una Midlet Java, permite el intercambio de las informaciones relativas a dicha por lo menos una aplicación 3 entre la interfaz gráfica de usuario 17 y el gestor de aplicaciones 5. Recupera y actualiza las informaciones relativas a las aplicaciones 3. Así, este conector 19 realiza la adaptación protocolaria apoyándose en protocolos, por ejemplo, basados en la JSR 177 (*Java Specification Request - Security and Trust Services API for J2ME*) para un diálogo con una tarjeta SIM o basado en la JSR 257 (*Java Specification Request - Contactless Communication API*) para una gestión de comunicación sin contacto.

Así, el medio de gestión centralizada 15 ofrece al usuario, por medio de la interfaz gráfica de usuario 17, las interfaces gráficas necesarias para la gestión de las aplicaciones 3 y para la construcción de una vista unificada de estas aplicaciones 3. La construcción de esta vista se efectúa apoyándose en el elemento conector 19 en relación con el gestor de aplicaciones 5 que ofrece todo un conjunto de funciones determinadas.

En efecto, según este ejemplo, el medio de acceso 7 del gestor de aplicaciones 5 ofrece a dicha por lo menos una aplicación 3 o al medio de gestión centralizada 15 por lo menos una función de entre un conjunto de funciones determinadas que comprenden las siguientes funciones:

- la selección de una aplicación 3 a partir de su identificador o de su índice,
- la grabación de una aplicación 3 y la grabación del identificador de esta aplicación en el medio de almacenamiento 9,
- la obtención del identificador de una aplicación 3 a partir de su índice,
- la actualización de ciertos parámetros de una aplicación 3 en relación con, por ejemplo, el nombre de la aplicación 3, la bandera (*flag*) de activación de un código de seguridad (código PIN) de la aplicación 3 o la bandera de activación de la propia aplicación 3,
- la recuperación de estos parámetros referentes al nombre de la aplicación 3, la bandera (*flag*) de activación del código de seguridad (código PIN) de la aplicación 3 o la bandera de activación de la aplicación 3,

- la recuperación de los datos de negocio de una aplicación 3, como por ejemplo un identificador de cliente, la fecha de validez de la aplicación 3, el crédito disponible,

- la recuperación de las transacciones relativas a una aplicación basándose en el registro de las transacciones,

- la verificación de un código de seguridad, por ejemplo el código PIN o una clave de autenticación basándose en el módulo de seguridad,

- la modificación de un parámetro de seguridad como el código PIN,

- la liberación de un código de seguridad como el código PIN,

- la autenticación de un dispositivo externo, por ejemplo durante el establecimiento de un canal seguro,

- la grabación de una transacción,

- la recuperación de un código de seguridad, por ejemplo el código PIN.

Por otra parte, el medio de almacenamiento 9 puede comprender, para una aplicación dada, el índice de la aplicación 3, el identificador de la aplicación 3, el nombre de la aplicación 3, el estado de la protección de la aplicación 3 por el código PIN (por ejemplo, el estado “verdadero” significa una verificación obligatoria del código PIN y un estado “falso” significa sin verificación del código PIN), y el estado de activación de la aplicación 3 (por ejemplo, el estado “verdadero” significa una aplicación activada y por lo tanto utilizable, y un estado “falso” significa una aplicación desactivada y por lo tanto no utilizable).

Además, el registro de transacciones 11 puede comprender las informaciones sobre todas las transacciones efectuadas por el usuario a partir de su terminal móvil. Una grabación de una transacción se puede definir mediante el identificador de la aplicación y de los datos significativos de la transacción (por ejemplo, la fecha de inicio de la transacción, la fecha del final de la transacción, el montante consumido, el montante que queda, el resultado de la transacción, etcétera).

Por otra parte, el módulo de seguridad 13 contiene y administra el código o códigos de seguridad de las aplicaciones (por ejemplo, el código PIN), el número máximo de intentos permitido antes de un bloqueo, el número de intentos errados sucesivamente así como la clave de desbloqueo PUK (*Pin Unblock Key*) del código PIN.

Así, el gestor de aplicaciones 5 puede gestionar los parámetros de las aplicaciones 3 (nombre, bandera de activación, etcétera), la grabación de las aplicaciones 3 y el rastro de las transacciones relativas a la utilización de las aplicaciones 3. Ofrece también funciones de consulta de los datos de negocio propio de cada aplicación, de gestión de los parámetros de seguridad (código PIN, verificación de código de seguridad, desbloqueo de código PIN), de lectura de las banderas de activación o incluso de grabación de una transacción. Dicho de otra manera, el gestor de aplicaciones 5 tiene conocimiento de las aplicaciones 3 instaladas en el terminal móvil así como de su parametrización.

Por consiguiente, el medio de gestión centralizada 15 en relación con el gestor de aplicaciones 5 permite que el usuario liste todas las aplicaciones 3 que están a su disposición, que liste las informaciones (en el sentido de datos de negocio) relativas a una aplicación 3 determinada, que seleccione una aplicación 3 particular y consulte su parametrización (entrada del código obligatorio o no, aplicación activada, etcétera), que consulte la lista de las últimas transacciones efectuadas con una aplicación 3, y que parametrice las aplicaciones (modificación del código PIN, activación de una aplicación, desactivación de una aplicación, activación de la protección por un código PIN, etcétera). Dicho de otra manera, el medio de gestión centralizada 15 puede gestionar, construir y visualizar la vista unificada de las aplicaciones 3 disponibles en el terminal móvil del usuario.

Por otra parte, se observará que cuando se ejecutan las aplicaciones 3 en el terminal móvil, permiten aportar un conjunto de servicios al usuario. La ejecución de una aplicación 3 puede estar vinculada a otra aplicación o incluso a un sistema externo al terminal (por ejemplo, la activación de una Cardlet por un lector local externo para un servicio de pago de una prestación). Se observará que cualquier aplicación 3 instalada y operativa en el terminal móvil es obligatoriamente conocida y está grabada con el gestor de aplicaciones 5. Así, cualquier aplicación nueva es grabada por el gestor de aplicaciones 5 en el medio de almacenamiento 9 del sistema de gestión 1 de las aplicaciones del terminal móvil.

Por otra parte, para realizar un servicio determinado, la aplicación 3 correspondiente recupera desde el gestor de aplicaciones 5 parámetros relativos a esta aplicación 3 con el fin de aportar una prestación al usuario.

La figura 4 ilustra un modo de realización particular del sistema de gestión 1 de las aplicaciones de un terminal móvil según la figura 3.

Este esquema ilustra un terminal móvil 21 de tipo JAVA que comprende un módulo de comunicación 23 (*Baseband*) que lleva a cabo las funciones básicas del terminal móvil 21, un módulo de identificación del abonado 25 (tarjeta SIM), un módulo de adaptación AML (*Adaptation and Mapping Layers*) 27, un módulo de comunicación local 29 (chip NFC), una antena 31, y un componente 33 correspondiente a una tarjeta SmartMX.

La tarjeta SmartMX es un componente 33 de tipo controlador de tarjeta chip (*smart card*) que combina coprocesadores de tipo DES (*Data Encryption Standard*) o RSA (Rivest Shamir Adleman) y que permite la implementación de sistemas operativos (OS) como el "Java Open Platform". Dispone también de interfaces ISO 14443 o ISO 7816 y almacena aplicaciones javacard (la aplicación "Cardlet Assistant") así como aplicaciones asociadas ("Cardlets Parner") y así como sus datos correspondientes. Por otra parte, el componente 33 (SmartMX) comprende un sistema operativo abierto 35 basado en el estándar JCOP (*JavaCardOpenPlatform*).

Así, el gestor de aplicación 5 se corresponde con el "Cardlet Assistant" y adopta la forma de una aplicación javacard denominada también CARDlet. Esta CARDlet 5 comprende cuatro subelementos que se corresponden con el medio de acceso 7, el medio de almacenamiento 9, el registro de transacciones 11 y el módulo de seguridad 13. Este gestor de aplicaciones 5 reside en este caso en el componente 33 (tarjeta SmartMX).

Por otra parte, las aplicaciones 3 se corresponden con aplicaciones JAVA de tipo javacard denominadas CARDlets (Cardlets asociadas) almacenadas en el componente 33 (tarjeta SmartMX).

El módulo de comunicación 23 (*Baseband*) comprende una interfaz hombre máquina 37 MMI (*Man Machine Interface*) nativa del terminal móvil 21, un módulo 39 de aplicaciones JAVA y un componente 41 que se corresponde con un Java 2 Micro Edition.

El módulo 39 de aplicaciones JAVA comprende una Midlet JAVA denominada "Card Summary" y que se corresponde con el medio de gestión centralizada 15. Así, esta Midlet JAVA que comprende la interfaz gráfica de usuario 17 y el conector 19, ofrece al usuario una vista unificada de las aplicaciones 3 (Cardlets).

El componente 41 (Java 2 Micro Edition) comprende todos los elementos necesarios para la ejecución de Mildets Java en el terminal móvil 21. Así, comprende una máquina virtual y las interfaces de programación de aplicaciones API (*Application Programming Interface*) necesarias para la ejecución de las MIDlets pero también las API que permiten dialogar con el módulo de identificación del abonado 25 (tarjeta SIM), con las aplicaciones 3 Java disponibles en el componente 33 (tarjeta SmartMX) o incluso con el módulo de comunicación local 29 (chip NFC) del terminal móvil 21.

El módulo de adaptación 27 (AML) comprende diferentes capas de abstracción, de adaptación y de correspondencia (*mapping*) que permiten una comunicación entre el módulo de comunicación 23 (*Baseband*) y en particular las Midlets, el componente 33 (tarjeta SmartMX) y el módulo de comunicación local 29 (chip NFC) del terminal móvil 21.

En efecto, el módulo de comunicación local 29 permite una comunicación local por medio de la antena 31 entre el terminal móvil 21 y un lector externo o entre el terminal móvil 21 y una etiqueta de RFID (*Radio Frequency IDentification*). El módulo de comunicación local 29 permite también la comunicación entre el medio de gestión centralizada 15 (Card Summary) y el gestor de aplicación 5 (Cardlet assistants) y las aplicaciones 3 (Cardlets partenaires).

Eventualmente, el módulo de identificación del abonado 25 (tarjeta SIM) puede comprender las aplicaciones 3' (representadas en líneas de puntos) de tipo CARDlets.

Se observará que el sistema de gestión 1 comprende uno o varios programas de ordenador que comprenden las instrucciones de código para realizar el procedimiento de gestión según la invención cuando el programa o programas de ordenador son ejecutados por los diferentes elementos del sistema de gestión 1 de las aplicaciones de un terminal móvil.

Las figuras 5 a 13 se corresponden con esquemas dinámicos que describen el funcionamiento entre los diferentes elementos del sistema de gestión 1 de las aplicaciones de un terminal móvil según la invención.

La figura 5 se corresponde con el lanzamiento o la activación, por parte del usuario 51, del medio de gestión centralizado 15. Ésta se realiza a partir de la interfaz hombre máquina 37 (IHM) del terminal móvil 21 (etapas E1, E2). La aplicación de gestión es lanzada entonces por la interfaz gráfica de usuario 17 que solicita la lista de las aplicaciones 3 disponibles o instaladas en el terminal móvil 21 con el medio de acceso 7 del gestor de aplicaciones 5 por medio del conector 19 (etapas E3, E4). Para ello, el medio de acceso 7 del gestor de aplicaciones 5 se dirige al medio de almacenamiento 9 (etapa E5). A cambio, la interfaz hombre máquina 37 recupera la lista de las aplicaciones disponibles en forma de una lista que contiene por lo menos los nombres e índices de las aplicaciones (etapas E6 a E9). Esta lista está entonces disponible en la interfaz hombre máquina (etapa E10).

La figura 6 se corresponde con la selección de una aplicación particular por parte del usuario 51.

En efecto, como consecuencia de la petición de selección de una aplicación particular por parte del usuario 51 por medio de la interfaz hombre máquina 37 (etapas E21, E22), la interfaz gráfica de usuario 17 del medio de gestión centralizada 15 transmite la petición al conector 19 (etapa E23). Este recupera entonces con el medio de acceso 7 del gestor de aplicaciones 5:

- el estado de activación de la aplicación 3, este estado de activación (activada/desactivada) se recupera con el medio de almacenamiento 9 (etapas E24 a E27).

- el estado de activación de la protección por código (por ejemplo código PIN) de la aplicación 3. Esta información también se recupera con el medio de almacenamiento 9 (etapas E28 a E31).

- la lista de las últimas transacciones en la aplicación 3 recuperadas con el registro de las transacciones 11 (etapas E32 a E35).

Todas estas informaciones son enviadas (etapa E36) por el conector a la interfaz gráfica de usuario 17 que las envía a la interfaz hombre máquina 37 (etapa E37) en donde estas informaciones que comprenden la lista de las últimas transacciones, el indicador de activación y el indicador de protección de código PIN en correspondencia con la aplicación son visualizadas (etapa E37) en la interfaz hombre máquina 37.

Con el fin de optimizar el tiempo de acceso y de tratamiento para futuras operaciones, la totalidad o partes de estas informaciones se pueden almacenar a nivel del conector 19. En este caso, cualquier solicitud posterior del medio de acceso 7 del gestor de aplicaciones 5 deja de ser sistemática.

La figura 7 se corresponde con la verificación de los parámetros de seguridad.

En efecto, cuando se requiere un código de seguridad (por ejemplo, un código PIN), el usuario 51 introduce su código por medio de la interfaz hombre máquina 37 (etapa E41). Éste es entonces transmitido al medio de acceso 7 del gestor de aplicaciones 5 a través del medio de gestión centralizada 15 que comprende la interfaz gráfica de usuario 17 y el conector 19 (etapa E42 a E44). La verificación es efectuada (etapa E45) por el módulo de seguridad 13 que, en caso de error, incrementa el contador del número de códigos falsos consecutivos. El módulo de seguridad 13 transmite el estado de verificación (verdadero/falso) a la interfaz hombre máquina 37 a través del medio de acceso 7, el conector 19 y la interfaz gráfica de usuario 17 (etapa E46 a E49).

Si se alcanza el número de tentativas de códigos falsos, la aplicación 3 se bloquea y el código queda inhabilitado. La liberación no puede ser llevada a cabo por un operador humano. Solo un sistema de seguridad externo 53 puede proceder a la liberación (PUK) del código (etapa E50) con el medio de acceso 7 del gestor de aplicaciones 5. Es significativo que cualquier fracaso durante esta fase acarrea el bloqueo definitivo del código. En la etapa E51, el medio de acceso 7 transmite el código de liberación al módulo de seguridad 13, que efectúa la verificación y, en caso de verificación positiva, desbloquea el código de seguridad; a continuación transmite el estado de verificación (verdadero/falso) al medio de acceso 7 (etapa E52), que a su vez lo transmite (etapa E53) al sistema de seguridad externo 53.

La figura 8 se corresponde con la petición, por parte del usuario 51, de la lista de las aplicaciones disponibles en el terminal móvil 21. En efecto, el usuario o cualquier otro sistema externo autorizado puede solicitar la lista de las aplicaciones disponibles en el terminal móvil.

Según este ejemplo, el usuario 51 solicita la lista de las aplicaciones a partir de la interfaz hombre máquina 37 del terminal móvil 21 (etapas E61, E62). Esta operación también puede ser llevada a cabo por la interfaz gráfica de usuario 17 con el fin de actualizar o “refrescar” la lista existente. Para ello, la interfaz gráfica de usuario 17 solicita la lista de las aplicaciones 3 disponibles o instaladas en el terminal móvil 21 con el medio de acceso 7 a través del conector 19 (etapas E63, E64). El medio de acceso 7 se dirige al medio de almacenamiento 9 (etapa E65). A cambio, la interfaz hombre máquina 37 recupera la lista de las aplicaciones disponibles bajo la forma de una lista que contiene por lo menos los nombres e índices de las aplicaciones (etapas E66 a E69). Esta lista queda entonces disponible en la interfaz hombre máquina 37 (etapa E70).

La figura 9 se corresponde con la actualización de los parámetros de una aplicación. Se observará que la actualización puede ser llevada a cabo para parámetros específicos de una aplicación o globales de todas las aplicaciones (por ejemplo, el código PIN si se desea un mismo código único para todas las aplicaciones).

Las etapas E80 a E88 se corresponden con la modificación del código de seguridad que puede referirse a una aplicación o a todas las aplicaciones.

En el caso de la modificación del código de seguridad para una aplicación 3 particular, el identificador de la aplicación es transmitido por el usuario 51 por medio de la interfaz hombre máquina 37, al mismo tiempo que el

código antiguo y el nuevo (etapa E80). La actualización de un código (global o no) requiere la verificación previa del código de seguridad.

Como consecuencia de la petición de cambio del código de seguridad por el usuario 51, la interfaz gráfica de usuario 17 recibe el mensaje de la interfaz hombre máquina 37 (etapa E81) y transmite, por medio del conector 19 al medio de acceso 7 del gestor de aplicaciones 5 (etapas E82, E83), el código nuevo, el código antiguo y, en el caso de la actualización del código de seguridad de una aplicación, el identificador de esta aplicación. El módulo de seguridad 13 recibe el mensaje (etapa E84) y verifica entonces la validez del código de seguridad a partir del código antiguo y a continuación, en caso del resultado positivo, procede a la actualización del código con la ayuda del código nuevo transmitido. El resultado de la modificación del código de seguridad (sí/no) es transmitido (etapas E85 a E88) por el módulo de seguridad 13 a la interfaz hombre máquina 37 por medio de los elementos 7, 19, y 17 respectivamente.

Las etapas E89 a E97 se corresponden con la activación de una aplicación.

Como consecuencia de una petición de activación de una aplicación por el usuario 51 por medio de la interfaz hombre máquina 37 (etapa E89), la interfaz gráfica de usuario 17 recibe el mensaje de la interfaz hombre máquina 37 (etapa E90) y transmite, por medio del conector 19 al medio de acceso 7 del gestor de aplicaciones 5 (etapas E91, E92), un identificador de la aplicación así como una variable de activación fijada a verdadera. Si la aplicación estaba desactivada, su activación se graba entonces en el medio de almacenamiento 9 (etapa E93). Si no, se devuelve un error para su visualización en la interfaz hombre máquina 37 del terminal móvil. En cualquier caso, el resultado de la activación (verdadero/falso) es transmitido (etapas E94 a E97) por el medio de almacenamiento 9 a la interfaz hombre máquina 37 a través de los elementos 7, 19, y 17 respectivamente.

Las etapas E98 a E106 se corresponden con la desactivación de una aplicación.

Como consecuencia de una petición de desactivación de una aplicación 3 por el usuario 51, por medio de la interfaz hombre máquina 37 (etapa E98), la interfaz gráfica de usuario 17 recibe el mensaje de la interfaz hombre máquina 37 (etapa E99) y transmite, por medio del conector 19, al medio de acceso 7 del gestor de aplicaciones 5 (etapas E100, E101), un identificador de la aplicación así como una variable de activación fijada a falso. Si la aplicación estaba activada, su desactivación se graba entonces en el medio de almacenamiento 9 (etapa E102). Si no, se devuelve un error para su visualización en la interfaz hombre máquina 37 del terminal móvil. En cualquier caso, el resultado de la desactivación (verdadero, falso) es transmitido (etapas E103 a E106) por el medio de almacenamiento 9 a la interfaz hombre máquina 37 a través de los elementos 7, 19, y 17 respectivamente.

Las etapas E107 a E115 se corresponden con la activación de la protección por un código de seguridad.

Como consecuencia de una petición de activación de una aplicación, de una lista de aplicaciones o de todas las aplicaciones por el usuario 51, por medio de la interfaz hombre máquina 37 (etapa E107), la interfaz gráfica de usuario 17 recibe el mensaje de la interfaz hombre máquina 37 (etapa E108) y transmite la petición de activación, a través del conector 19 al medio de acceso 7 del gestor de aplicaciones 5 (etapas E109, E110). La ausencia de parámetros indica que la activación se refiere a todas las aplicaciones. La petición de activación para una o varias aplicaciones se realiza precisando en el requerimiento la lista de las aplicaciones que se desea proteger. En los dos casos, la petición contiene una variable de activación de la protección fijada a verdadera. La petición es entonces procesada por el medio de almacenamiento 9 (etapa E111), que verifica la posibilidad de la activación (función ya activada, aplicación inexistente, etcétera) antes de cualquier materialización. El resultado de la activación (verdadero/falso) es transmitido (etapas E112 a E115) por el medio de almacenamiento 9 a la interfaz hombre máquina 37 a través de los elementos 7, 19, y 17 respectivamente.

Las etapas E116 a E124 se corresponden con la desactivación de la protección por un código de seguridad.

Como consecuencia de una petición de desactivación de una aplicación, de una lista de aplicaciones o de todas las aplicaciones por el usuario 51, a través de la interfaz hombre máquina 37 (etapa E116), la interfaz gráfica de usuario 17 recibe el mensaje de la interfaz hombre máquina 37 (etapa E117) y transmite la petición de desactivación, por medio del conector 19, al medio de acceso 7 del gestor de aplicaciones 5 (etapas E118, E119). La ausencia de parámetros indica que la desactivación se refiere a todas las aplicaciones. La petición de desactivación para una o varias aplicaciones se efectúa precisando en el requerimiento la lista de las aplicaciones que ya no se desea proteger. En los dos casos, la petición contiene una variable de activación de la protección fijada a falsa. La petición a continuación es procesada por el medio de almacenamiento 9 (etapa E120), que verifica la posibilidad de desactivación (función ya desactivada, aplicación inexistente, etcétera) antes de cualquier materialización. El resultado de la desactivación (verdadero/falso) es transmitido (etapas E121 a E124) por el medio de almacenamiento 9 a la interfaz hombre máquina 37 a través de los elementos 7, 19 y 17 respectivamente.

La figura 10 se corresponde con una recuperación de los parámetros de una aplicación. Este esquema muestra que es posible recuperar los parámetros de una aplicación 3 o todos los datos relativos a una o al conjunto de las aplicaciones 3 del usuario. Los parámetros y datos son aquellos contenidos en el medio de almacenamiento 9, el registro de transacciones 11 o el módulo de seguridad 13.

Las etapas E131 a E136 se corresponden con la recuperación del estado de activación de una aplicación. La interfaz gráfica de usuario 17 recupera con el medio de acceso 7 del gestor de aplicaciones 5, a través del conector 19, el estado de activación de una aplicación a partir de su identificador o de su índice. La petición es procesada por el medio de almacenamiento 9, que devuelve el estado de activación (activada/desactivada) de la aplicación.

Así, la interfaz gráfica de usuario 17 transmite esta petición, por medio del conector 19, al medio de acceso 7 del gestor de aplicaciones 5 (etapas E131, E132). La petición es entonces procesada por el medio de almacenamiento 9 (etapa E133), que transmite el estado (activado/desactivado) a la interfaz gráfica de usuario 17 por medio de los elementos 7 y 19 respectivamente (etapas E134 a E136).

Las etapas E137 a E142 se corresponden con la recuperación del estado de la protección por un código PIN de la aplicación. La interfaz gráfica de usuario 17 recupera con el medio de acceso 7 del gestor de aplicaciones 5 a través del conector 19, el estado de protección por código (por ejemplo, por código PIN) de una aplicación, a partir de su identificador o de su índice. La petición es procesada por el medio de almacenamiento 9, que devuelve el estado de protección por código (por ejemplo, por código PIN) de la aplicación (activado/desactivado).

Así, la interfaz gráfica de usuario 17 transmite esta petición, a través del conector 19 al medio de acceso 7 del gestor de aplicaciones 5 (etapas E137, E138). La petición es entonces procesada por el medio de almacenamiento 9 (etapa E139), que transmite el estado (activado/desactivado) a la interfaz gráfica de usuario 17 por medio de los elementos 7 y 19 respectivamente (etapas E140 a E142).

Las etapas E143 a E148 se corresponden con la recuperación de la lista de las transacciones de una aplicación 3 a partir de su nombre o de su índice. Así, la interfaz gráfica de usuario 17 transmite esta petición, a través del conector 19, al medio de acceso 7 del gestor de aplicaciones 5 (etapas E143, E144). La petición es entonces procesada por el registro de transacción 11 (etapa E145), que transmite a continuación la lista de las últimas transacciones para la aplicación a la interfaz gráfica de usuario 17 por medio de los elementos 7 y 19 respectivamente (etapas E146 a E148).

Las etapas E149 a E154 se corresponden con la recuperación del identificador de una aplicación 3. Así, la interfaz gráfica de usuario 17 transmite esta petición, a través del conector 19, al medio de acceso 7 del gestor de aplicaciones 5 (etapas E149, E150). La petición es entonces procesada por el medio de almacenamiento 9 (etapa E151), que transmite entonces el identificador único de la aplicación a la interfaz gráfica de usuario 17 por medio de los elementos 7 y 19 respectivamente (etapas E152 a E154).

La figura 11 se corresponde con la recuperación de los datos de negocio de una aplicación. Esto permite recuperar los datos de negocio de una aplicación tales como el identificador del cliente, la fecha de validez de la aplicación, el crédito disponible, el tipo de suscripción, etcétera. Estos datos son gestionados por la propia aplicación 3, por contraposición a los parámetros de la aplicación que son gestionados en el nivel del medio de almacenamiento 9, del registro de transacciones 11 o del módulo de seguridad 13. Para este requerimiento, es la aplicación 3 la que se invoca directamente y no el gestor de aplicaciones 5.

Como consecuencia de una petición de visualizar los datos de negocios relativos a una aplicación 3, del usuario 51 por medio de la interfaz hombre máquina 37 (etapas E161, E162), la interfaz gráfica de usuario 17 recupera, a partir del identificador de la aplicación, la lista de estos datos directamente de la aplicación 3 a través del conector 19 del medio de gestión centralizada 15 (etapas E163 a E167). Previamente la aplicación 3 debe haber sido seleccionada por el conector 19 (etapa E164). Si la aplicación no existe (identificador inexistente), en la interfaz hombre máquina 37 se puede visualizar un mensaje del tipo “Aplicación Desconocida”.

Según una variante, la recuperación de datos de negocio de una aplicación 3 se puede efectuar por remisión al medio de acceso 7 del gestor de aplicaciones 5.

La figura 12 ilustra la grabación de una aplicación en el terminal móvil. Como consecuencia de una descarga exitosa de una aplicación 3 en el terminal móvil, el elemento o la aplicación (por ejemplo, una Midlet Java) responsable de la descarga (de referencia 61) graba la aplicación 3 con el medio de acceso común 7 del gestor de aplicaciones 5 (etapa E171). Este último graba entonces la aplicación 3 con el medio de almacenamiento 9 (etapa E172). Las etapas E173 y E174 indican si la grabación ha resultado exitosa (sí/no). Así, esta grabación permite ofrecer al usuario una vista unificada de sus aplicaciones.

La figura 13 ilustra la utilización de una aplicación. En efecto, durante la provisión de una prestación a un usuario, las aplicaciones van a invocar al gestor de aplicaciones 5 con el fin de recuperar informaciones sobre su parametrización. Al finalizar la realización de una prestación, el gestor de aplicaciones 5 es invocado también para grabar la transacción.

Las etapas E181 a E184 se corresponden con la lectura de la bandera de activación de la aplicación 3. En efecto, de forma previa a cualquier utilización de un servicio, la lectura (etapa E181) de la bandera de activación permite saber

si la aplicación 3 asociada al servicio en el terminal móvil del usuario está o no activada. Así, el medio de acceso 7 del gestor de aplicaciones 5 se dirige (etapa E182) al medio de almacenamiento 9 poseedor de esta información. El medio de almacenamiento 9 envía (etapas E183, E184) a la aplicación 3 el estado de activación (verdadero/falso).

Las etapas E185 a E188 se corresponden con la lectura de la bandera de activación del código PIN. En efecto, de forma previa a cualquier utilización de un servicio, la lectura (etapa E185) de la bandera de activación del código PIN permite saber si se requiere una fase de verificación de un código de seguridad. Así, el medio de acceso 7 del gestor de aplicaciones 5 se dirige (etapa E186) al medio de almacenamiento 9 poseedor de esta información. El medio de almacenamiento 9 envía (etapas E187, E188) a la aplicación 3 el estado de activación del código PIN (verdadero/falso).

Las etapas E189 a E192 se corresponden con la recuperación (etapa E189) del código PIN que permite que una aplicación autorizada recupere el código PIN del usuario para la aplicación referida. Así, el medio de acceso 7 del gestor de aplicaciones 5 se dirige (etapa E190) al módulo de seguridad 13 poseedor de esta información. El módulo de seguridad 13 envía (etapas E191, E192) a la aplicación 3 el código PIN solicitado.

Las etapas E193 a E196 se corresponden con la grabación de una transacción. En efecto, al finalizar una prestación, la aplicación 3 graba la transacción en el registro de transacciones 11, a través del medio de acceso 7 del gestor de aplicaciones 5 (etapas E193, E194). Durante esta fase, la aplicación 3 precisa su identificador (o su índice) así como informaciones que constituyen la transacción. Preferentemente, estas informaciones comprenden por lo menos el identificador del usuario, el tipo de la transacción, el estado de la transacción (sí/no), la fecha suministrada por la aplicación, la duración y el montante si así fuera necesario.

REIVINDICACIONES

1. Sistema de gestión de por lo menos una aplicación que comprende un terminal móvil (21) y por lo menos una tarjeta (33) en la cual está grabada dicha por lo menos una aplicación, en el que la tarjeta comprende un gestor de aplicaciones (5) apto para gestionar dicha por lo menos una aplicación y el terminal móvil comprende un medio de gestión centralizada (15) apto para comunicarse con el gestor de aplicaciones (5) de la tarjeta con el fin de intercambiar informaciones relativas a dicha por lo menos una aplicación de la tarjeta,

comprendiendo el gestor de aplicaciones (5) de la tarjeta (33) un medio de almacenamiento (9) que permite la grabación de informaciones relativas a dicha por lo menos una aplicación,

caracterizado porque el gestor de aplicaciones (5) de la tarjeta (33) comprende además un registro de transacciones (11) apto para grabar informaciones relativas a las transacciones realizadas por el usuario sobre dicha por lo menos una aplicación.

2. Sistema según la reivindicación 1, caracterizado porque el medio de gestión centralizada del terminal comprende:

- unos medios de interfaz gráfica de usuario (17), y

- unos medios de conexión (19) aptos para intercambiar informaciones relativas a dicha por lo menos una aplicación entre los medios de interfaz gráfica de usuario (17) y el gestor de aplicaciones de la tarjeta.

3. Tarjeta (33) que comprende por lo menos una aplicación y un gestor de aplicaciones (5) apto para intercambiar informaciones relativas a dicha por lo menos una aplicación con un terminal móvil,

comprendiendo el gestor de aplicaciones (5) un medio de almacenamiento (9) que permite la grabación de informaciones relativas a dicha por lo menos una aplicación,

caracterizada porque el gestor de aplicaciones (5) comprende además un registro de transacciones (11) apto para grabar informaciones relativas a las transacciones realizadas por el usuario sobre dicha por lo menos una aplicación.

4. Tarjeta según la reivindicación 3, caracterizada porque el gestor de aplicaciones (5) comprende además un módulo de seguridad (13) apto para administrar datos de seguridad relativos a dicha por lo menos una aplicación.

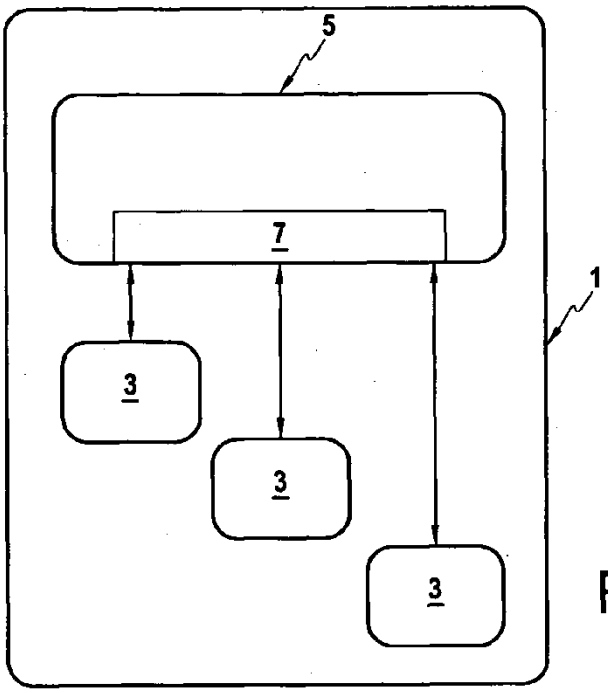


FIG.1

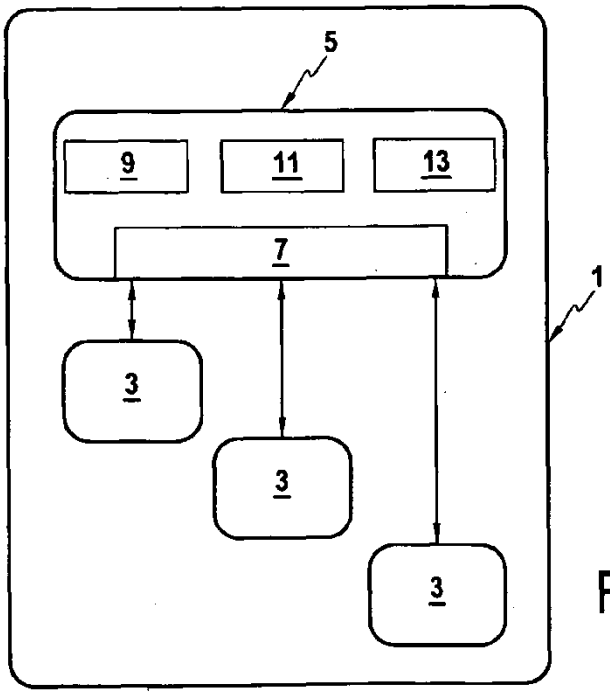


FIG.2

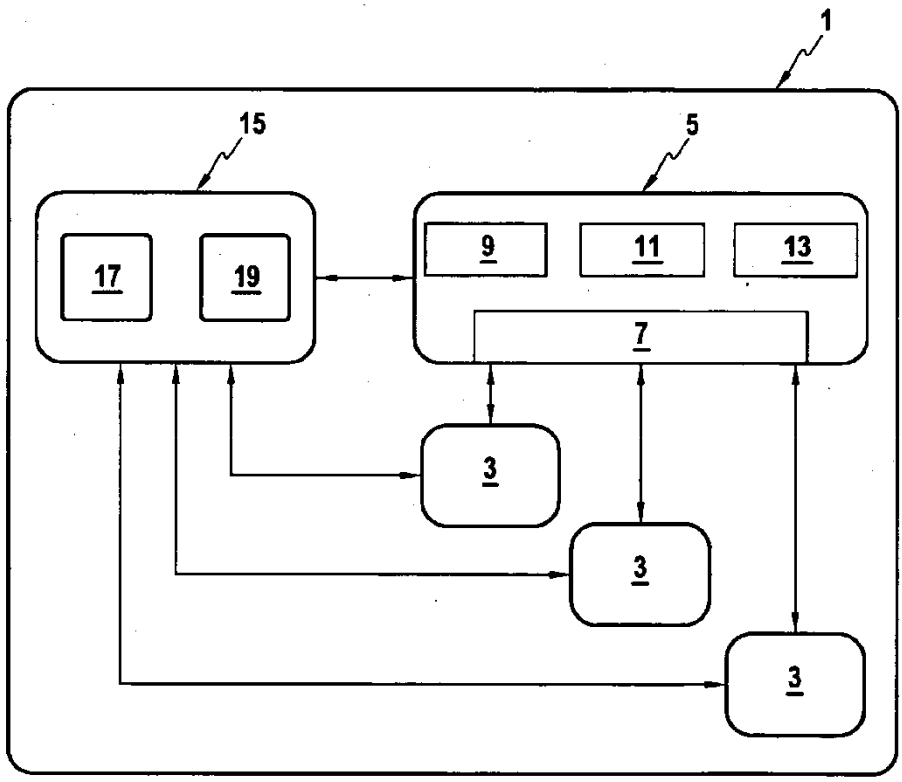


FIG.3

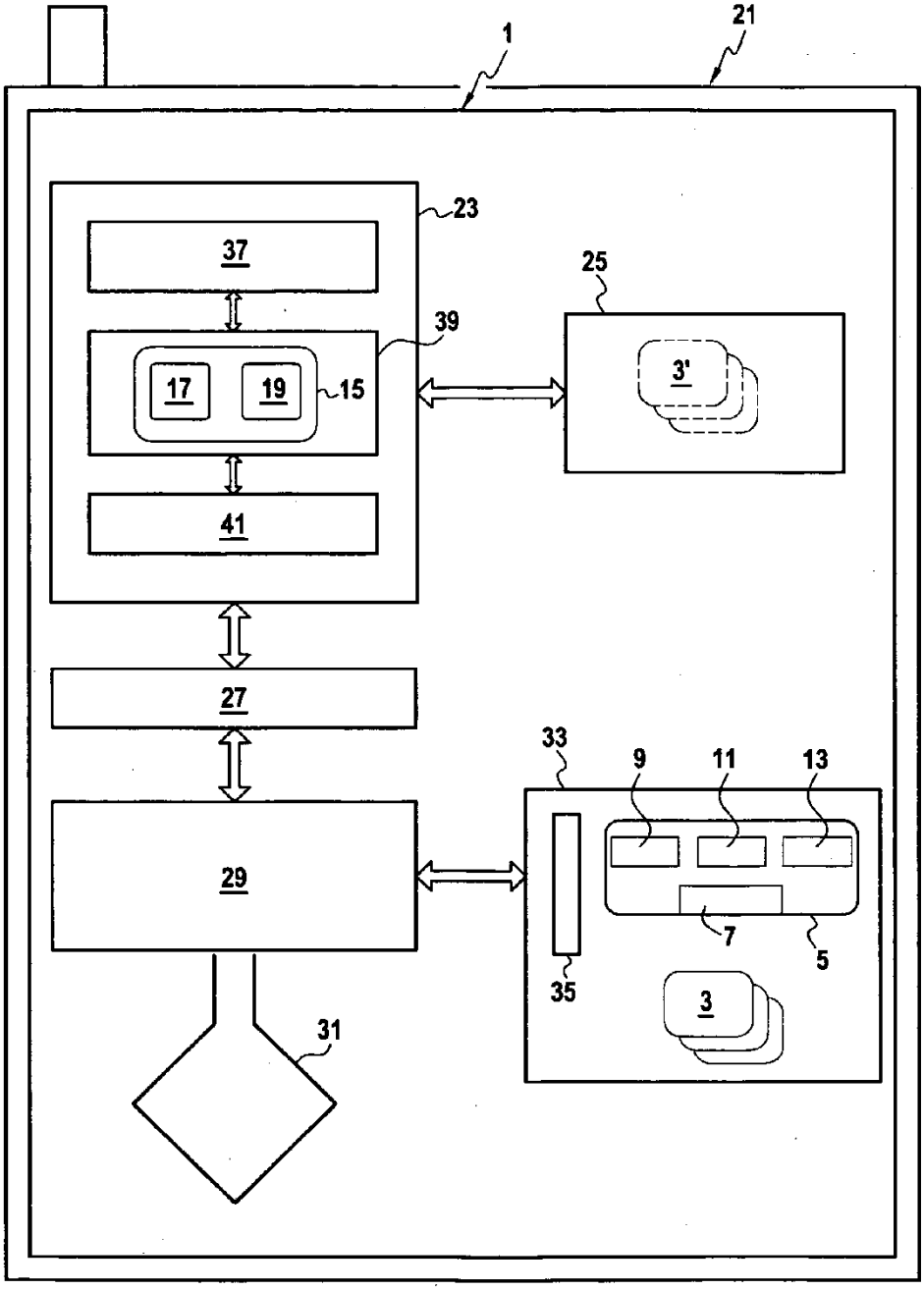


FIG.4

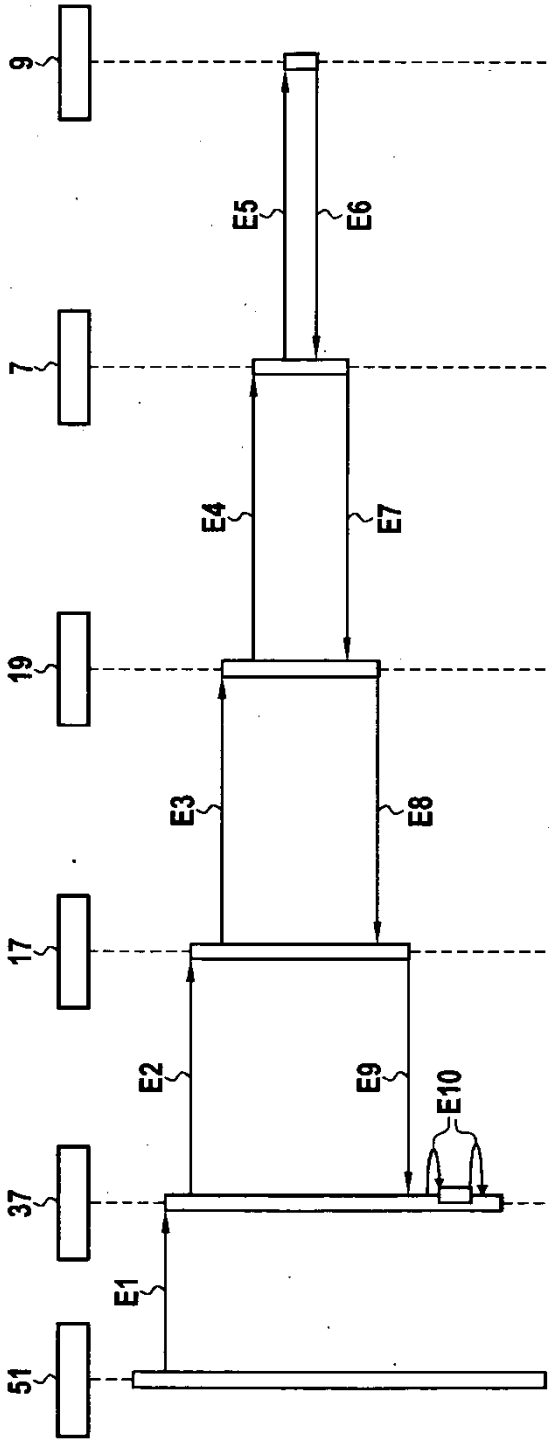


FIG.5

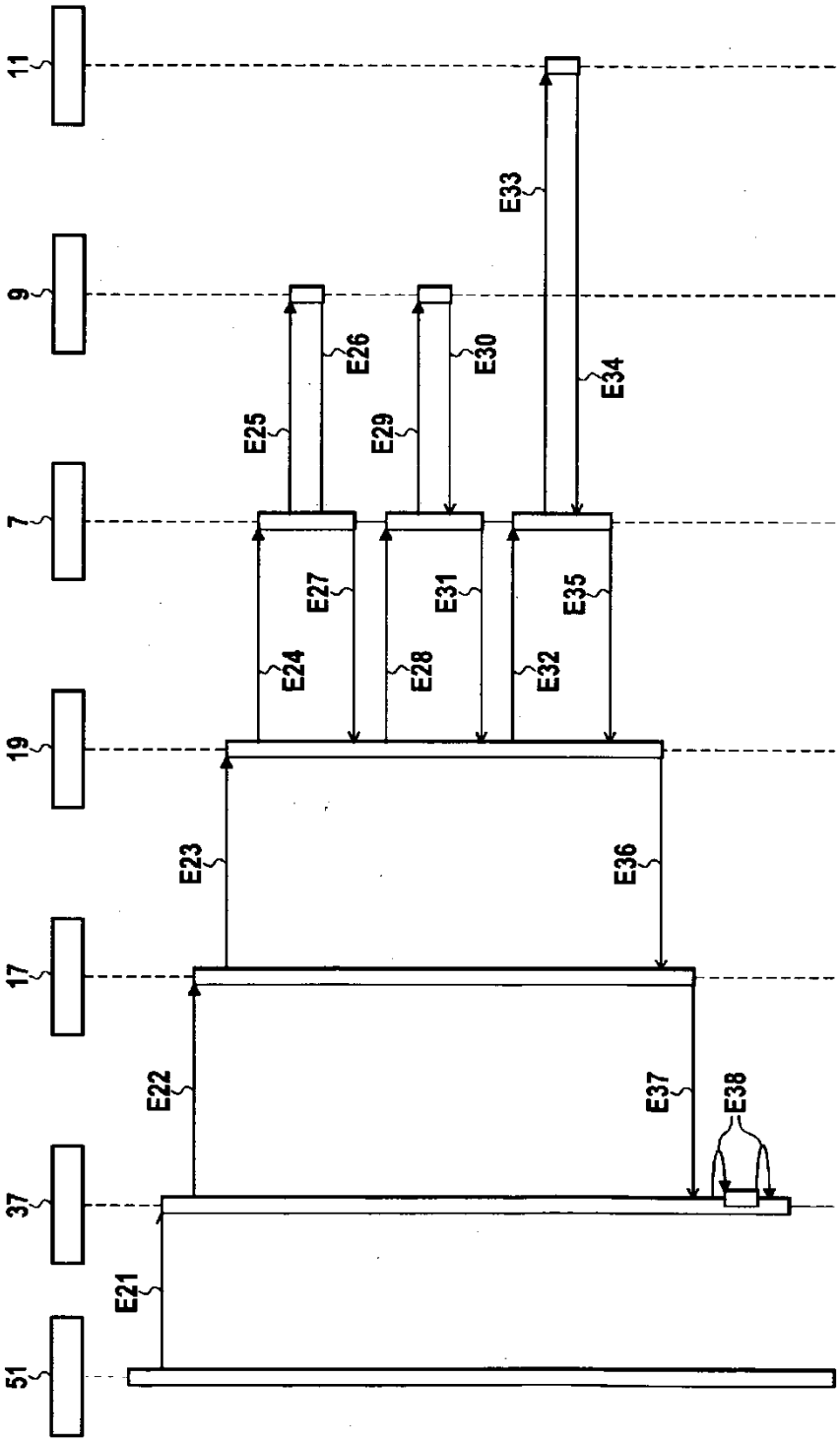

11
9
7
19
17
37
51
E21
E22
E23
E24
E25
E26
E27
E28
E29
E30
E31
E32
E33
E34
E35
E36
E37
E38

FIG.6

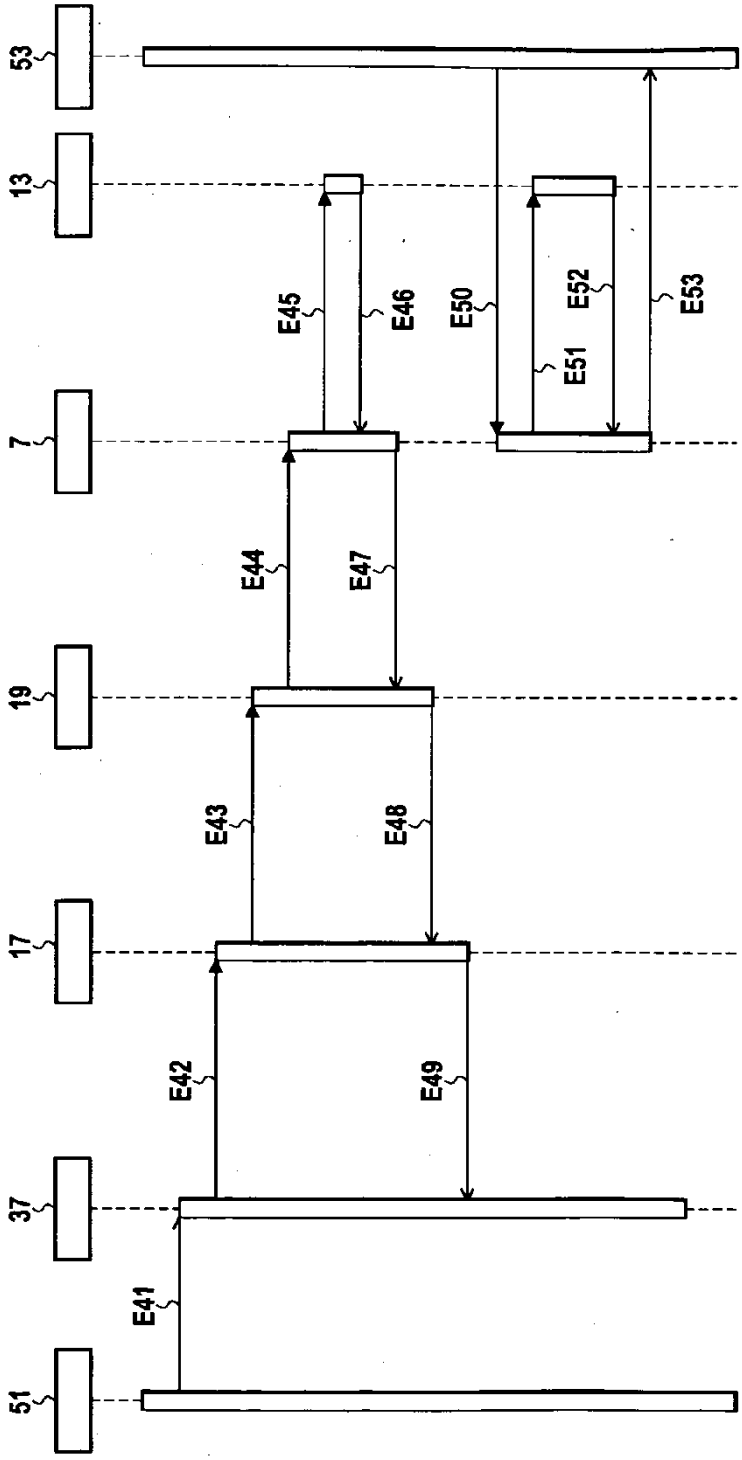

53
13
7
19
17
37
51
E41
E42
E43
E44
E45
E46
E47
E48
E49
E50
E51
E52
E53

FIG.7

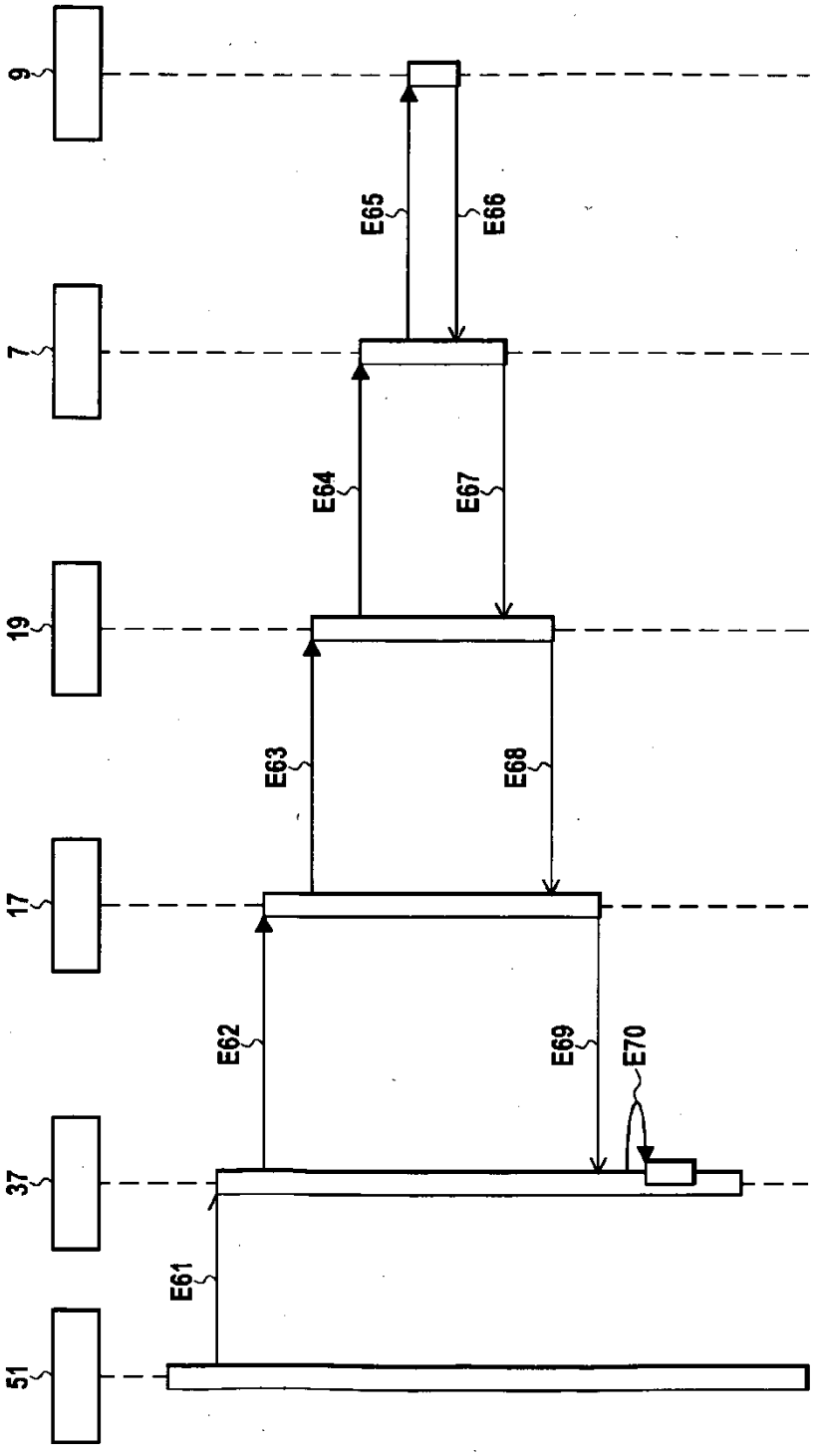


FIG.8

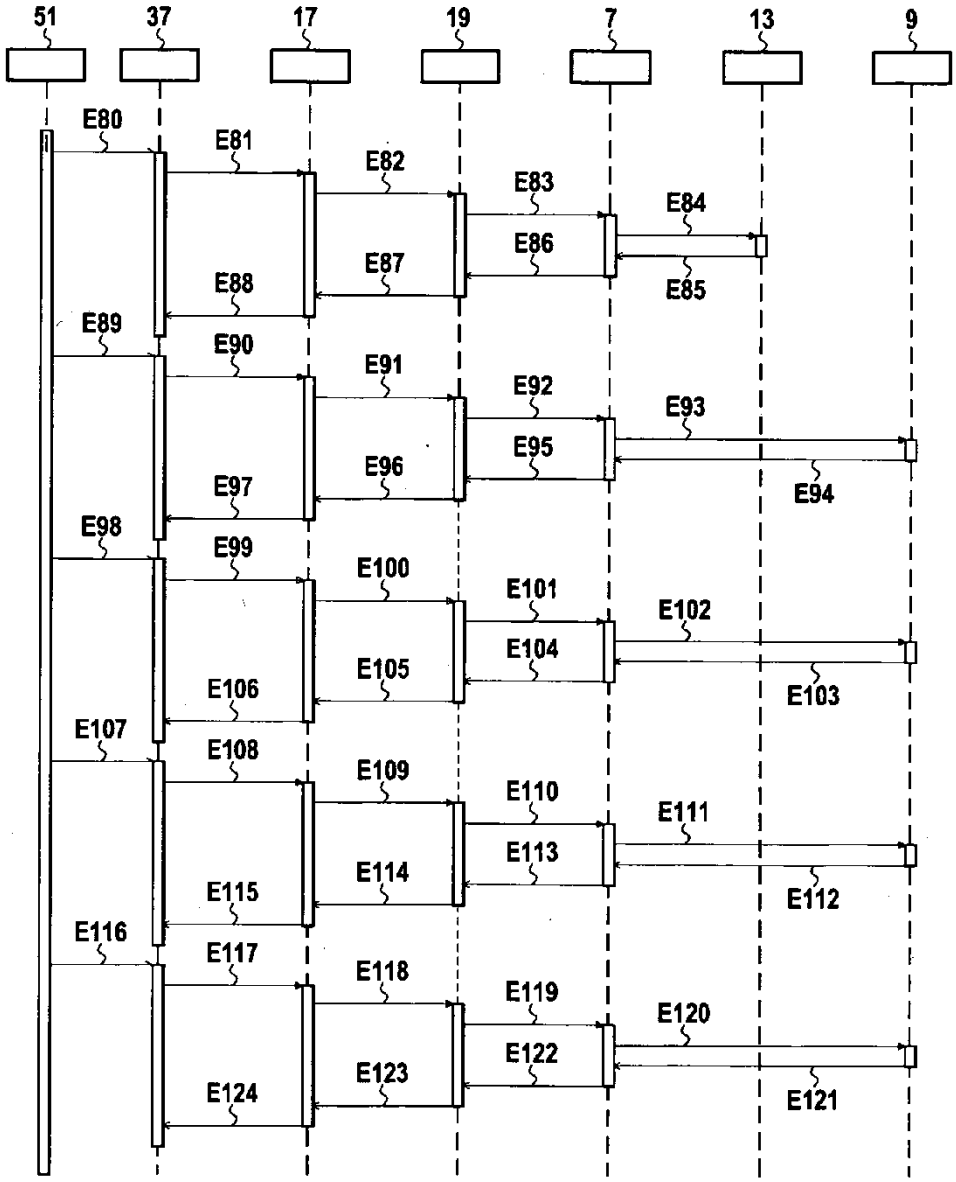
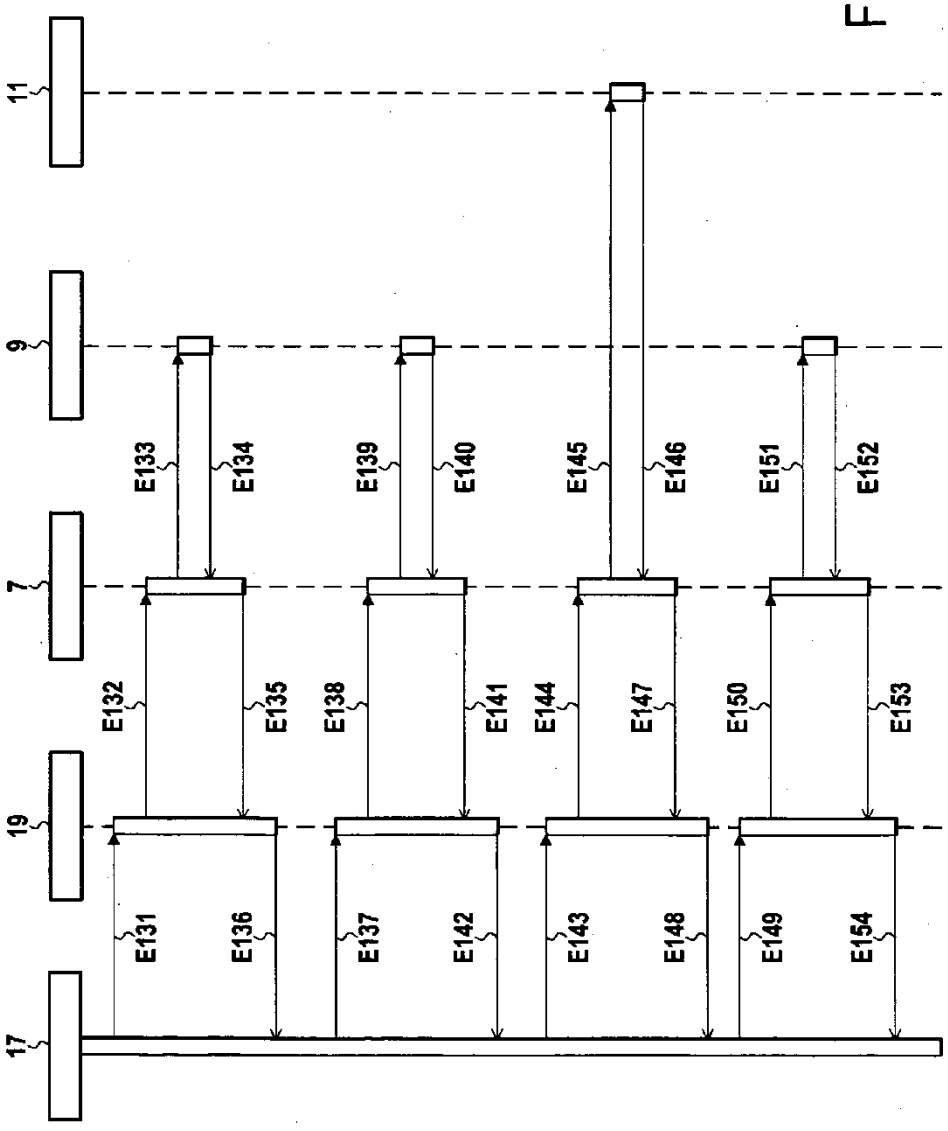

51
37
17
19
7
13
9
E80
E81
E82
E83
E84
E85
E86
E87
E88
E89
E90
E91
E92
E93
E94
E95
E96
E97
E98
E99
E100
E101
E102
E103
E104
E105
E106
E107
E108
E109
E110
E111
E112
E113
E114
E115
E116
E117
E118
E119
E120
E121
E122
E123
E124

FIG.9

FIG.10


11
9
7
19
17
E131
E132
E133
E134
E135
E136
E137
E138
E139
E140
E141
E142
E143
E144
E145
E146
E147
E148
E149
E150
E151
E152
E153
E154

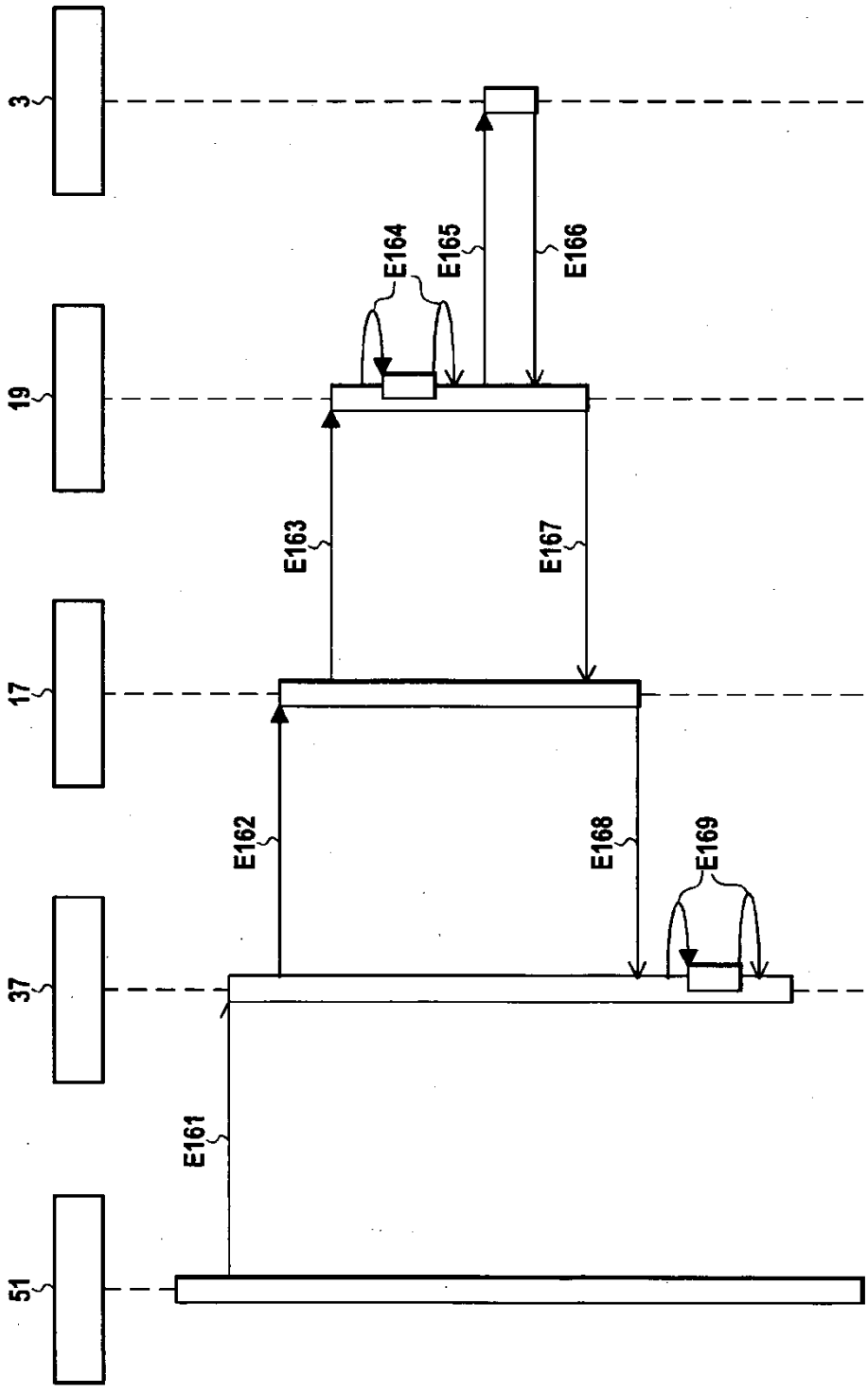


FIG.11

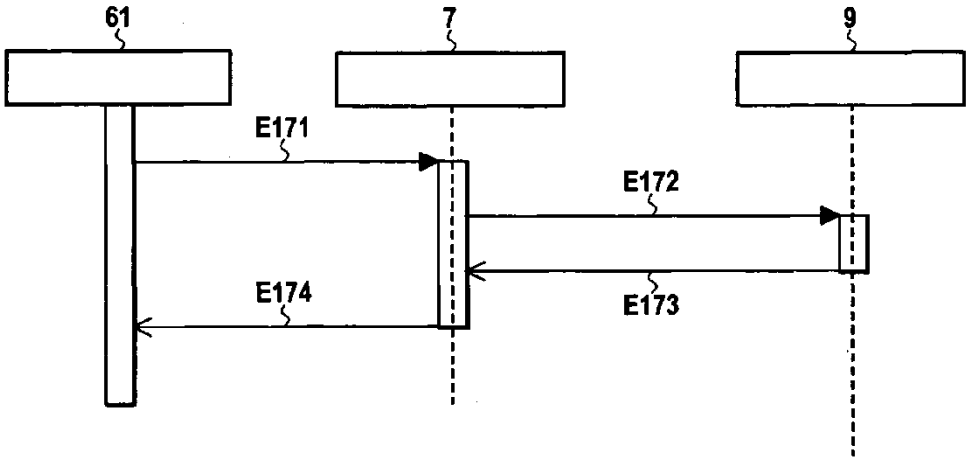


FIG.12

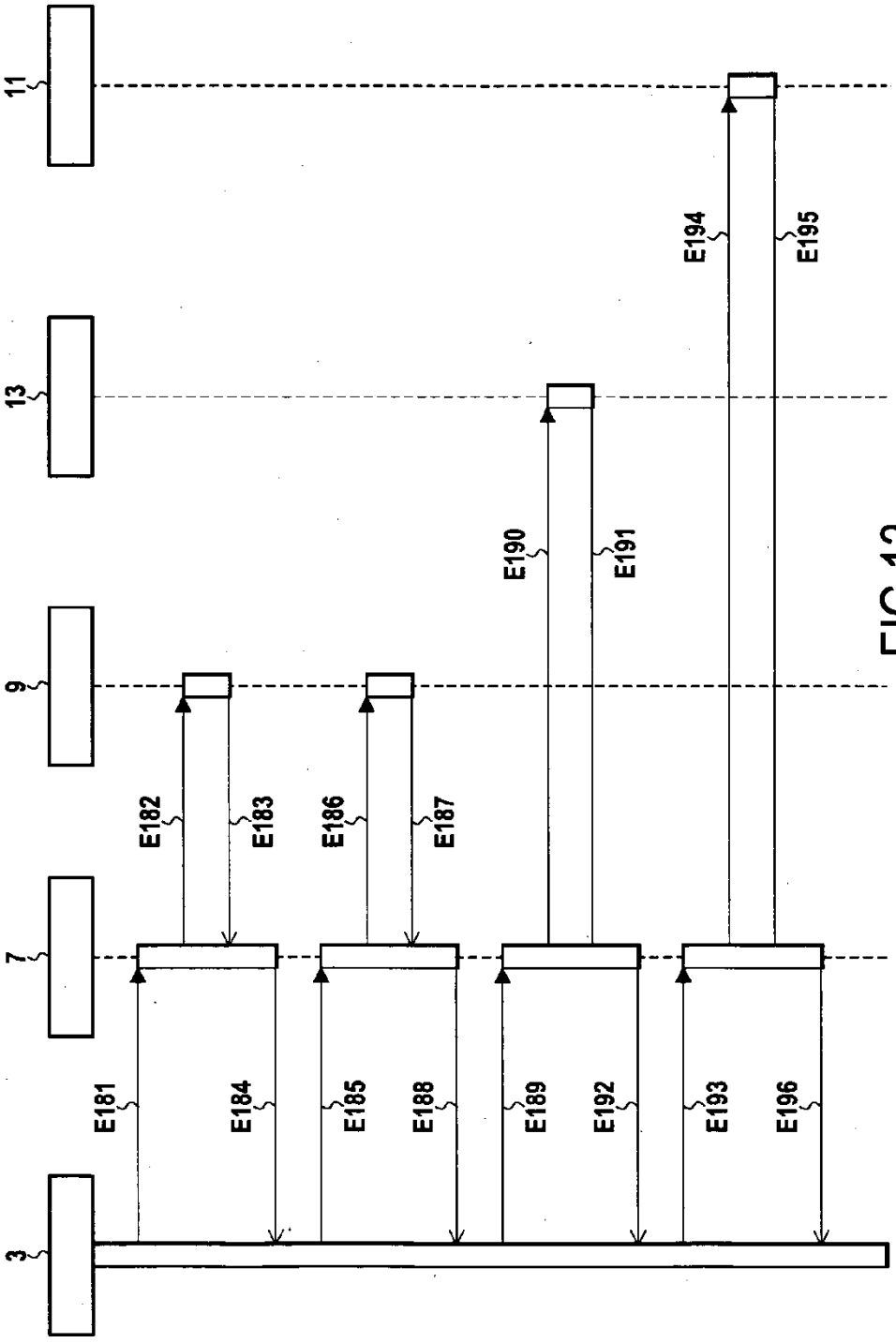

11
13
9
7
3
E181
E182
E183
E184
E185
E186
E187
E188
E189
E190
E191
E192
E193
E194
E195
E196

FIG.13