(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 718 322**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 21/74 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.11.2015 E 15192654 (0)**

(97) Fecha y número de publicación de la concesión europea: **02.01.2019 EP 3018609**

(54) Título: **Procedimiento de carga de archivo en memoria de acceso aleatorio en un aparato electrónico y aparato electrónico asociado**

(30) Prioridad:

05.11.2014 FR 1460679

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.07.2019

(73) Titular/es:

IDEMIA FRANCE (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

FRANCOIS, AXEL y
SARTORI, MICHELE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento de carga de archivo en memoria de acceso aleatorio en un aparato electrónico y aparato electrónico asociado

Ámbito técnico al cual se refiere la invención

La presente invención se refiere a la partición de archivos entre un entorno de ejecución de confianza y un entorno de ejecución polivalente.

La invención se refiere más particularmente a un procedimiento de carga de archivo en memoria de acceso aleatorio en un aparato electrónico concebido para funcionar en un entorno de ejecución de confianza y en un entorno de ejecución polivalente, así como a dicho aparato electrónico.

La invención se aplica particularmente ventajosamente en el caso en que se prevé una zona de memoria particionada utilizable a la vez por el entorno de ejecución de confianza y por el entorno de ejecución polivalente.

Antecedente tecnológico

Como se ha explicado por ejemplo en el artículo "*The Untapped Potential of Trusted Execution Environments on Mobile Devices"* de J.-E. Ekberg, K. Kostiainen et N. Asokan *in* IEEE Security & Privacy, volumen PP edición 99, 16 Abril 2014, es conocido asegurar el funcionamiento de los aparatos electrónicos por la utilización de un sistema de explotación de confianza (o "Trusted OS" según la denominación anglo-sajona), que permite proporcionar un entorno de ejecución de confianza (o TEE por "*Trusted Execution Environment")* en el cual algunas aplicaciones solamente pueden ser instaladas y ejecutadas.

Un entorno de confianza de este tipo es generalmente propuesto junto con un entorno polivalente (o REE por "*Rich Execution Environment")* en el cual las obligaciones de seguridad son menores y un mayor número de aplicaciones pueden por consiguiente ser instaladas. El entorno polivalente se basa en la ejecución en el seno del aparato electrónico de un sistema de explotación polivalente (o "*Rich OS"* según la denominación anglo-sajona), distinto del sistema de explotación de confianza.

Con el fin de garantizar un buen aislamiento entre los dos entornos de ejecución y de este modo una buena seguridad de funcionamiento, se prevén en general espacios de memoria expresos para cada entorno de ejecución, particularmente en memoria de acceso aleatorio.

Se ha propuesto no obstante utilizar además una zona de memoria particionada accesible por los dos entornos de ejecución, como se ha mencionado particularmente en la presentación "*Next Generation Mobile Rootkits"* de T. Roth BlackHat Europe 2013 (citada como referencia [15] en el artículo mencionado anteriormente). El artículo de Li Xiaolei et al.: "DroidVault: A Trusted Data Vault for Android Devices", 19th international conference on engineering of complex computer systems, 2014, propone el concepto de "trusted data vault", una pequeña herramienta de confianza que gestiona con toda seguridad el almacenado y la utilización de datos sensibles en un aparato móvil no fiable.

Objeto de la invención

La invención está definida por las reivindicaciones adjuntas. En este contexto, la presente invención propone un procedimiento de carga de archivo en memoria de acceso aleatorio en un aparato electrónico concebido para funcionar en un entorno de ejecución de confianza, debido a la ejecución de un sistema de explotación de confianza por un procesador del aparato electrónico, o en un entorno de ejecución polivalente, caracterizado por que comprende las etapas siguientes:

- recepción, por el sistema de explotación de confianza, de informaciones que identifican al menos un archivo;
- comprobación, por el sistema de explotación de confianza, de la conformidad del archivo identificado con al menos un criterio dado;
- en caso de conformidad, carga (por ejemplo por el sistema de explotación de confianza) del archivo identificado en una zona de memoria de acceso aleatorio accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente.

El sistema de explotación de confianza controla así la carga de los archivos en una zona de la memoria de acceso aleatorio particionada entre el entorno de ejecución de confianza y el entorno de ejecución polivalente; esta zona particionada es accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente y los archivos que son memorizados allí, utilizados particularmente durante el funcionamiento en el entorno de ejecución de confianza, no podrán por consiguiente ser alterados por una aplicación ejecutada en el entorno de ejecución polivalente.

Este procedimiento de carga puede ser realizado en la puesta en funcionamiento del aparato electrónico, como se describe con detalle más adelante, o en el transcurso del funcionamiento, por ejemplo, en el momento del lanzamiento (en el entorno de ejecución polivalente) de una aplicación correspondiente al archivo o utilizando el archivo.

El archivo identificado es por ejemplo una aplicación, una biblioteca o un conjunto de datos.

Según otras características opcionales y por consiguiente no limitativas:

- las informaciones que identifican el archivo están contenidas en una descripción de requisitos (por ejemplo una lista de requisitos) preparada durante el funcionamiento en el entorno de ejecución polivalente;
- la descripción de requisitos se elabora en función de los datos representativos de las frecuencias de utilización de las aplicaciones instaladas en el entorno de ejecución polivalente;
- la descripción de requisitos se elabora en función de las estadísticas de utilización relacionadas con varios criterios;
- el procedimiento comprende una etapa de construcción, por el sistema de explotación de confianza, de una lista de partición que incluye una designación del archivo cargado y una dirección de memorización del archivo cargado (por ejemplo, una dirección virtual como se indica a continuación);
- la lista de partición incluye una información de comprobación de integridad asociada con el archivo cargado;
- la lista de partición incluye un certificado generado por el sistema de explotación de confianza y relacionado con el archivo cargado;
- la lista de compartición se memoriza en la mencionada zona de memoria de acceso aleatorio en lectura solo durante el funcionamiento en el entorno de ejecución polivalente;
- la indicada carga se realiza a partir de una memoria no volátil (por ejemplo una memoria no volátil reprogramable);
- la mencionada zona es accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente por medio de direcciones virtuales que apuntan en direcciones físicas distintas de las direcciones virtuales en cuestión;
- las informaciones que identifican el archivo son recibidas durante una conmutación del entorno de ejecución polivalente al entorno de ejecución de confianza.

El procedimiento puede además comprender las etapas siguientes, ejecutadas en el entorno de ejecución polivalente para cada archivo mencionado en el descriptivo de requisitos:

- determinación si el mencionado archivo es cargado en la indicada zona de memoria de acceso aleatorio accesible en lectura solo;
- en caso negativo, carga del archivo en cuestión en otra zona de la memoria de acceso aleatorio accesible en escritura durante el funcionamiento en el entorno de ejecución polivalente.

El procedimiento propuesto puede además comprender las etapas siguientes:

- a continuación de una instalación de una nueva aplicación en el entorno de ejecución polivalente, transmisión al sistema de explotación de confianza de un descriptivo de requisitos puesto al día;
- carga, en la zona de memoria de acceso aleatorio accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente, de un nuevo archivo designado en el descriptivo de requisitos actualizado.

La invención propone igualmente un aparato electrónico que comprende al menos un procesador y una memoria de acceso aleatorio, y concebido para funcionar en un entorno de ejecución de confianza, debido a la ejecución de un sistema de explotación de confianza por el procesador, o en un entorno de ejecución polivalente, caracterizado por que el sistema de explotación de confianza está concebido para recibir informaciones que identifican al menos un archivo, para comprobar la conformidad del archivo identificado con al menos un criterio dado y para cargar, en caso de conformidad, el archivo identificado en una zona de la memoria de acceso aleatorio accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente.

Este dispositivo electrónico puede comprender además una o varias de las características opcionales formuladas más arriba en términos de procedimiento.

Descripción detallada de un ejemplo de realización

La descripción que sigue respecto a los dibujos adjuntos, dados a título de ejemplos no limitativos, hará comprender mejor en qué consiste la invención y cómo puede ser realizada.

En los dibujos adjuntos:

- la figura 1 representa los elementos principales de un aparato electrónico utilizado en el marco de la invención;
- la figura 2 representa esquemáticamente la utilización de dos entornos de ejecución en el seno del aparato electrónico de la figura 1;
- la figura 3 ilustra la partición de la memoria de acceso aleatorio propuesta dentro del marco de la invención;
- la figura 4a representa tablas funcionales memorizadas en el seno del aparato electrónico de la figura 1 y utilizadas dentro del marco de la presente invención;
- la figura 4b representa una tabla tridimensional de memorización de estadísticas de utilización utilizable en una variante de realización;
- la figura 5 representa un ejemplo de procedimiento de carga de archivos en la memoria de acceso aleatorio conforme a la invención;
- la figura 6 representa listas funcionales elaboradas en el transcurso del procedimiento de la figura 5.

La figura 1 representa los elementos principales de un aparato electrónico 10 en el cual se realiza la invención.

Este aparato electrónico 10, aquí un terminal (por ejemplo de tipo teléfono inteligente o "*smarphone"* según la denominación anglo-sajona), comprende una arquitectura a base de microprocesador. En variante, el aparato electrónico podría ser un decodificador de video (a veces llamado por la denominación anglo-sajona "*set-top box"*) o un aparato electrónico conectado (tal como una pulsera, un reloj, gafas o un contador de pasos).

El aparato electrónico 10 incluye un procesador 2, por ejemplo un microprocesador de un sistema en microcircuito (o SoC por *"System on Chip")*. Además del procesador 2, un sistema de microcircuito comprende otros elementos electrónicos con diversas funcionalidades, por ejemplo una memoria de lectura solamente (no representada), o ROM por "*Read Only Memory"*, una memoria de acceso aleatorio 4 – o RAM por "*Random Access Memory"* – y una memoria no volátil programable 6, por ejemplo de tipo EEPROM por "*Electrically Erasable and Programmable Read Only Memory"*).

La figura 2 representa esquemáticamente la utilización de dos entornos de ejecución en el seno del aparato electrónico 10.

Para ello, dos sistemas de explotación distintos pueden ser ejecutados por el procesador 2 del aparato electrónico 10: un sistema de explotación polivalente 20 (o "*Rich OS"* según la denominación anglo-sajona) y un sistema de explotación de confianza 30 (o "*Trusted OS"*), a veces denominado sistema de explotación de seguridad ("*Secure OS"*).

El sistema de explotación polivalente 20 permite la telecarga, la instalación y la ejecución de aplicaciones con una gran libertad para el usuario. La utilización del sistema de explotación polivalente 20 crea así un entorno polivalente o REE (por "*Rich Execution Environment"*).

Por el contrario, dentro del marco del funcionamiento del aparato electrónico 10 sobre la base del sistema de explotación de confianza 30, las posibilidades de telecarga y de instalación de aplicaciones están limitadas (por ejemplo para aplicaciones que han recibido una certificación particular) de forma que la utilización del sistema de explotación de confianza permita crear en el seno del aparato electrónico 10 un entorno de ejecución de confianza o TEE (por "*Trusted Execution Environment"*).

Este entorno de ejecución de confianza ofrece por ejemplo un nivel de seguridad conforme a los criterios comunes EAL (por "*Evaluation Assurance Level"*), que corresponde a la norma ISO 15408, con un nivel comprendido entre 2 y 7, o a la norma FIPS (por "*Federal Information Processing Standard")* 140-2.

El aparato electrónico 10 utiliza igualmente un monitor de seguridad 40 (o "*Secure Monitor"* según la denominación anglo-sajona), que puede ser ejecutado por procesador 2 del aparato electrónico 10. El monitor de seguridad 40 controla la conmutación entre el funcionamiento del aparato electrónico 10 sobre la base del sistema de explotación polivalente 20 y el funcionamiento del aparato electrónico 10 sobre la base del sistema de explotación de confianza 30 (y viceversa), de forma que el aparato electrónico 10 funcione en cada instante sobre la base de uno solo de los dos sistemas de explotación 20, 30 (es decir, en uno solo de los dos entornos mencionados anteriormente). El funcionamiento del monitor de seguridad 40 responde a las mismas exigencias de seguridad que el sistema de explotación de confianza 30 y se considera por consiguiente en general que el monitor de seguridad forma parte del entorno de ejecución de confianza TEE, como se ha representado en la figura 2.

Según un modo de realización que se puede considerar, el sistema de explotación ejecutado antes de la conmutación (por ejemplo el sistema de explotación polivalente 20) se pone en reserva por la conmutación y cualquier acceso a elementos externos al procesador (por ejemplo la interfaz hombre-máquina que comprende particularmente un teclado y/o una pantalla y/u otro módulo de entrada-salida) es entonces inhibido por el sistema de explotación en reserva, de forma que el sistema de explotación activado por la conmutación (aquí el sistema de explotación de confianza 30) controle totalmente el elemento externo, aquí la interfaz hombre-máquina.

El monitor de seguridad 40 puede igualmente permitir, en la conmutación, el paso de informaciones del sistema de explotación ejecutado antes de la conmutación al sistema de explotación ejecutado después de la conmutación, como se ha ilustrado en el ejemplo de procedimiento de carga de archivos en memoria de acceso aleatorio presentado más adelante.

En el ejemplo descrito aquí, el sistema de explotación polivalente 20 y el sistema de explotación de confianza 30 son ejecutados por el procesador 2 del aparato electrónico 10. Se podría en variante utilizar un aparato electrónico que comprenda dos procesadores, siendo ejecutado el sistema de explotación polivalente 20 en uno y siendo el sistema de explotación de confianza 30 ejecutado en el otro.

La figura 3 representa la partición de la memoria de acceso aleatorio 4 en tres zonas Z1, Z2, Z3 utilizada dentro del marco de la presente invención.

Una primera zona Z1 de la memoria de acceso aleatorio 4 es accesible en lectura y en escritura por el sistema de explotación de confianza 30 solamente. El sistema de explotación polivalente 20, y por consiguiente las aplicaciones ejecutadas en el entorno polivalente REE, no tienen acceso a la primera zona Z1.

Se prevé por ejemplo que la primera zona Z1 sea accesible por el sistema de explotación de confianza 30 con direcciones comprendidas en un primer margen P1 de direcciones, aquí direcciones cuyo octeto de peso fuerte está comprendido entre h00 y h0F (significando la indicación hxy que el número xy es expresado en indicación hexadecimal). Estas direcciones corresponden por ejemplo a las direcciones físicas en la memoria de acceso aleatorio 4.

Una segunda zona Z2 de la memoria de acceso aleatorio 4 es una zona particionada utilizada a la vez por el sistema de explotación de confianza 30 y por el sistema de explotación polivalente 20. Precisamente, la segunda zona Z2 es accesible en lectura y en escritura por el sistema de explotación de confianza 30; la segunda zona Z2 es por el contrario accesible en lectura solo por el sistema de explotación polivalente 20. El sistema de explotación polivalente 20, e igualmente las aplicaciones ejecutadas en el entorno polivalente REE, no pueden por consiguiente escribir en la segunda zona Z2.

Se prevé por ejemplo que la segunda zona Z2 sea accesible por el sistema de explotación de confianza 30 con direcciones comprendidas en una segunda zona P2 de direcciones, aquí direcciones cuyo octeto de peso fuerte está comprendido entre h10 y h1F. Estas direcciones corresponden por ejemplo a las direcciones físicas en la memoria de acceso aleatorio 4. La segunda zona Z2 es por el contrario accesible (en lectura solamente) a partir del sistema de explotación polivalente 20 por medio de direcciones comprendidas en un tercer margen P3 de direcciones, distinta del segundo margen P2 de direcciones, aquí direcciones cuyo octeto de peso fuerte está comprendido entre h20 y h2F.

Una tercera zona Z3 de la memoria de acceso aleatorio 4 está prevista para la utilización por el sistema de explotación polivalente 20 (y las aplicaciones ejecutadas en el entorno polivalente REE). Esta tercera zona Z3 es por consiguiente accesible en lectura y en escritura por el sistema de explotación polivalente 20 y, a través de éste, por las aplicaciones ejecutadas en el entorno polivalente REE.

Aunque la utilización de la tercera zona Z3 por el sistema de explotación de confianza 30 no esté prevista en funcionamiento normal, se puede prever que el sistema de explotación de confianza 30 tenga la posibilidad de acceder a la tercera zona Z3 en lectura y/o en escritura. Las restricciones impuestas a las aplicaciones ejecutadas en el entorno de confianza TEE (por ejemplo, en términos de certificación) permiten en efecto garantizar que los accesos a la tercera zona Z3 a partir del entorno de confianza TEE serán limitados a casos excepcionales, por ejemplo, cuando el conjunto de la memoria de acceso aleatorio 4 deba ser reinicializada por un motivo de seguridad. Así, el sistema de explotación de confianza 30 puede por ejemplo leer datos relacionados con el usuario (nombre, información de interfaz, etc.) en la tercera zona Z3. La escritura de datos en la tercera zona Z3 estará en cuando a la misma limitada en casos específicos (por ejemplo en peticiones particulares y/o en estados de funcionamiento particulares del sistema de explotación de confianza 30).

Se prevé por ejemplo que la tercera zona Z3 sea accesible por el sistema de explotación polivalente 20 con direcciones comprendidas en un cuarto margen P4 de direcciones distinta del tercer margen P4 de direcciones; el cuarto margen P4 de direcciones corresponde aquí a las direcciones cuyo octeto de peso fuerte está comprendido entre h00 y h1F. En los casos en que la tercera zona Z3 sea accesible a partir del sistema de explotación de confianza 30, los accesos pueden ser realizados por medio de direcciones comprendidas en un quinto margen P5 de direcciones, distinto de los primero y segundo márgenes P1, P2 de direcciones, aquí direcciones cuyo octeto de peso fuerte está comprendido entre h20 y h3F. Estas últimas direcciones corresponden por ejemplo a las direcciones físicas en la memoria de acceso aleatorio 4.

Se observa que las segunda y tercera zonas Z2, Z3 son accesibles por el sistema de explotación polivalente 20 (y por consiguiente para las aplicaciones ejecutadas en el entorno polivalente REE) con direcciones (virtuales) distintas de las direcciones físicas en la memoria de acceso aleatorio 4, por ejemplo gracias a la utilización de alias, lo cual

permite particionar la memoria de acceso aleatorio 4 entre las diferentes zonas Z1, Z2, Z3 e impedir cualquier acceso a la primera zona Z1 mediante aplicaciones ejecutadas en el entorno polivalente REE, permitiendo a tales aplicaciones acceder en lectura solamente a la segunda zona Z2.

La figura 4a representa las tablas funcionales memorizadas dentro del aparato electrónico 10, por ejemplo en la memoria no volátil reprogramable 6.

Una primera tabla T1 memoriza, para cada aplicación APPL1, APPL2, APPL3 instalada en el entorno de ejecución polivalente REE un dato representativo de la frecuencia de utilización de la aplicación en cuestión. Este dato representativo de la frecuencia de utilización es por ejemplo el número de utilizaciones de la aplicación en un periodo de tiempo dado, aquí un periodo de tiempo de una semana. En variante, se podría contar el número de utilizaciones en un lapso de tiempo de duración variable, definido por ejemplo por medio de un criterio distinto del criterio temporal, tal como un criterio relacionado con un ciclo de carga o de descarga de una batería que quipa el aparato electrónico.

Las diferentes aplicaciones APPL1, APPL2, APPL3 instaladas pueden así ser clasificadas por frecuencia de utilización decreciente, por ejemplo dentro de la primera tabla T1 como se ha representado en la figura 4a.

En variante, se podrían utilizar tablas multidimensionales (por ejemplo tridimensionales como se ha representado en la figura 4b) con el fin de memorizar estadísticas de utilización según varios criterios. Se memoriza así por ejemplo para cada aplicación APPLi, como se ha representado en la figura 4b, una estadística de utilización S (por ejemplo una frecuencia de utilización) en función del momento T (hora y día de la semana por ejemplo) y del lugar L.

En este caso, las diferentes aplicaciones APPLi pueden clasificarse por frecuencia de utilización decreciente utilizando las estadísticas relacionadas con el momento T en la semana correspondiente al momento actual y al lugar L correspondiente al lugar actual.

Una segunda tabla T2 memoriza, para cada aplicación APPL1, APPL2, APPL3 instalada en el entorno de ejecución polivalente REE, los diferentes recursos (o archivos) utilizados por la aplicación en cuestión en el transcurso de su ejecución; estos recursos son por ejemplo bibliotecas de funciones LIB1, LIB2, LIB3 o conjuntos(o archivos) de datos DAT1, DAT2, DAT4, DAT6.

Las aplicaciones instaladas en el aparato electrónico 10 (para utilización en el entorno de ejecución polivalente REE en lo que respecta a las aplicaciones APPL1, APPL2, APPL3 mencionadas anteriormente), así como los recursos que las mismas utilizan (aquí las funciones LIB1, LIB2, LIB3 y los datos DAT1, DAT2, DAT4, DAT6), se memorizan en memoria no-volátil reprogramable 6 (por ejemplo después de su telecarga de un ordenador distante, tal como un servidor distribuidor de servicios, gracias a los medios de telecomunicación no representados del aparato electrónico 10).

Las aplicaciones que deben ser ejecutadas por el procesador 2 (así como eventualmente al menos una parte de los recursos que la aplicación puede utilizar) son no obstante cargadas en la memoria de acceso aleatorio 4, después de la selección de la aplicación por el usuario, o antes como se explica a continuación con el fin de hacer más rápido la emisión de la aplicación.

La figura 5 representa un ejemplo de procedimiento de carga de archivos en memoria de acceso aleatorio 4 en la puesta en funcionamiento del aparato electrónico 10.

Este procedimiento comienza por una etapa E0 de inicialización del aparato electrónico 10 como consecuencia de su arranque (por ejemplo debido a su activación por el usuario). Después de esta etapa de inicialización E0, todos los octetos de la memoria de acceso aleatorio 4 tienen en general un valor predeterminado (por ejemplo h00 o hFF), debido a la concepción física de la memoria de acceso aleatorio 4 o de una sub-etapa de reinicialización forzada comprendida en la etapa de inicialización E0.

La etapa de inicialización E0 comprende otras sub-etapas necesarias para la inicialización del funcionamiento del aparato electrónico 10, por ejemplo la carga, de la memoria no-volátil reprogramable 6 en la memoria de acceso aleatorio 4, del sistema de explotación de confianza 30 y el lanzamiento de su ejecución.

La etapa de inicialización E0 es seguida de una etapa E2 en el transcurso de la cual el sistema de explotación de confianza 30 comanda la carga, en la primera zona Z1 de la memoria de acceso aleatorio 4, de archivos (aplicaciones y recursos utilizados por esta, particularmente bibliotecas y datos) utilizados en el marco del entorno de ejecución de confianza TEE. En el modo de realización descrito aquí, los archivos son cargados (es decir copiados) en la primera zona Z1 a partir de la memoria no-volátil reprogramable 6 (donde han sido previamente instalados como ya se ha indicado).

La memorización correcta de los archivos en la primera zona Z1 es eventualmente comprobada por el sistema de explotación de confianza 30, por ejemplo, por la espera de un indicador de buen funcionamiento procedente de la

memoria de acceso aleatorio 4 (eventualmente acompañado de una suma de control de los datos escritos en memoria) y/o lectura de los datos escritos para comparación con los datos a escribir.

Las aplicaciones cargadas en la primera zona Z1 en la etapa E2 son por ejemplo aplicaciones que utilizan funcionalidades de base (tales como las relacionadas con la seguridad del funcionamiento del aparato electrónico 10) o aplicaciones frecuentemente utilizadas en el funcionamiento del aparato electrónico 10 dentro del marco del entorno de ejecución de confianza TEE.

El procedimiento se continua en la etapa E4 en la cual el sistema de explotación de confianza 30 emite una petición REQ con destino al sistema de explotación polivalente 20 con el fin de obtener una lista de requisitos y transmitirla al sistema de explotación polivalente 20. Como ya se ha indicado, la transmisión de informaciones (aquí la petición REQ) y la conmutación del sistema de explotación de confianza 30 al sistema de explotación polivalente 20 se realiza por ejemplo por medio del monitor de seguridad 40.

El sistema de explotación polivalente 20 es por consiguiente ejecutado por el procesador 2 en la etapa E6 (por ejemplo después de haber sido cargado en memoria de acceso aleatorio 4 por el monitor de seguridad 40) y recibe la petición REQ emitida por el sistema de explotación de confianza 30 en la etapa E4.

El sistema de explotación polivalente 20 prepara entonces en la etapa E7 la lista de requisitos L1 solicitada, que indica como se ha explicado a continuación los archivos (aplicaciones y recursos utilizados por estas aplicaciones, particularmente bibliotecas y datos) cuya utilización dentro del marco del entorno de ejecución polivalente REE es previsible.

Para ello, el sistema de explotación polivalente 20 consulta por ejemplo la primera tabla T1 con el fin de determinar la aplicación más frecuentemente utilizada (o sea aquí la aplicación APPL2), luego consulta la segunda tabla T2 con el fin de determinar los recursos utilizados por esta aplicación (aquí las bibliotecas LIB1, LIB3 y el archivo de datos DAT1).

Las referencias a los archivos así determinados (a saber la aplicación más frecuentemente utilizada APPL2 y los recursos LIB1, LIB3, DAT1 utilizados por esta aplicación) son entonces añadidos a la lista de requisitos L1.

Este proceso puede eventualmente ser repetido para otras aplicaciones, por ejemplo por orden decreciente de frecuencia de utilización, hasta que el tamaño de memoria correspondiente a los archivos relacionados en la lista de requisitos L1 llega a un umbral predefinido (por ejemplo igual al tamaño de la segunda zona Z2 de memoria de acceso aleatorio 4) o, en variante, para todas las aplicaciones instaladas para utilización en el entorno de ejecución polivalente REE.

En el caso de la figura 6, una referencia a la aplicación APPL3 y a los recursos LIB2, DAT2 es así añadida a la lista de requisitos L1. (Se observa que no se añade de nuevo a la lista de requisitos L1 una referencia a un archivo ya mencionado en la lista de requisitos L1, aquí la biblioteca LIB3).

En el caso en que ninguna estadística de utilización esté disponible (como por ejemplo en la primera puesta en servicio del aparato electrónico 10), el sistema de explotación polivalente 20 utiliza por ejemplo como lista de requisitos L1 una lista por defecto (memorizada con este fin en memoria no-volátil reprogramable 6).

El sistema de explotación polivalente 20 emite la lista de requisitos L1 con destino al sistema de explotación de confianza 30 en la etapa E8. Como ya se ha indicado anteriormente, esta transferencia de información es aquí gestionada por el monitor de seguridad 40 y va acompañada de la conmutación del funcionamiento del aparato electrónico del entorno de ejecución polivalente REE al entorno de ejecución de confianza TEE.

La ejecución del sistema de explotación de confianza 30 retoma por consiguiente en la etapa E10, con recepción de la lista de requisitos L1.

El sistema de explotación de confianza 30 determina entonces en la etapa E11, para cada archivo referenciado en la lista de requisitos L1, si este archivo es compatible con una carga en la zona de memoria particionada (o segunda zona) Z2, comprobando la conformidad del archivo con ciertos criterios, aquí uno al menos de los criterios siguientes:

- el archivo es susceptible de ser utilizado en el entorno de ejecución de confianza TEE (lo cual es el caso cuando el archivo está certificado y/o ha sido instalado –es decir cargado en memoria no volátil reprogramable 6- por el sistema de explotación de confianza 30);
- la utilización de este (mismo) archivo por una parte en el funcionamiento en el entorno de confianza TEE y por otra parte en el funcionamiento en el entorno de ejecución polivalente REE es permitida (algunos archivos que pueden ser especificados como reservados para una utilización en el entorno de ejecución de confianza TEE y por consiguiente prohibidos de utilizar en el entorno de ejecución polivalente REE, por ejemplo, archivos que requieren un alto nivel de seguridad).

En la práctica, el sistema de explotación de confianza 30 determina por ejemplo si un archivo es compatible con una carga en la zona de memoria particionada Z2 por medio de un indicador (o indicación binaria) contenido en un lugar expreso del archivo en cuestión, tal como los indicadores previstos en los sistemas de derecho utilizados por algunos sistemas de explotación.

En el ejemplo descrito aquí con referencia a la figura 6, la aplicación APPL2 es una aplicación instalada durante el funcionamiento del aparato electrónico 10 en el entorno de ejecución polivalente REE, sin certificación, y la biblioteca LIB2 es una biblioteca de funciones criptográficas (por ejemplo de cifrado, de descifrado y/o de firma electrónica) de la cual no se desea que pueda ser utilizada algunas veces en el marco del entorno de ejecución de confianza TEE y algunas veces en el marco del entorno de ejecución polivalente REE. De forma general, una biblioteca de este tipo que necesita un nivel de seguridad elevado es certificada y su utilización implica un control de su integridad.

El sistema de explotación de confianza 30 determina por consiguiente en este ejemplo en la etapa E11 que los archivos siguientes puedan ser cargados en la segunda zona Z2 de memoria viva 4: LIB1, LIB3, DAT1, APPL3, DAT2.

El sistema de explotación de confianza 30 calcula en la etapa E12 una suma de control global relacionada con estos archivos para cargar en la segunda zona Z2.

El sistema de explotación de confianza 30 puede entonces proceder en la etapa E13 a la carga, en la segunda zona Z2, de los archivos determinados en la etapa E11 (aquí los archivos LIB1, LIB3, DAT1, APPL3, DAT2). Estos archivos son aquí cargados a partir de la memoria no-volátil reprogramable 6 (es decir copiados de la memoria no-volátil reprogramable 6 a la segunda zona Z2 de la memoria de acceso aleatorio 4 bajo el control del sistema de explotación de confianza 30).

La memorización correcta de los archivos en la segunda zona Z2 es eventualmente comprobada por el sistema de explotación de confianza 30, por ejemplo por espera de un indicador de buen funcionamiento procedente de la memoria de acceso aleatorio 4 (eventualmente acompañado de una comprobación de la suma de control de los datos escritos en memoria, calculada como se ha indicado anteriormente en la etapa E12) y/o lectura de los datos escritos para comparación con los datos a escribir. En variante, en lugar de utilizar una suma de control global relacionada con el conjunto de archivos a cargar como se ha propuesto anteriormente, se puede utilizar una suma de control por archivo a cargar.

Se puede prever por otro lado que el sistema de explotación de confianza 30 libere, en la primera zona Z1, espacios de memoria donde han sido cargados en la etapa E2 archivos de los cuales una copia ha sido cargada en la segunda zona Z2 en la etapa E13. Durante el funcionamiento en el entorno de ejecución de confianza TEE, estos archivos podrán en efecto ser consultados o ejecutados por lectura en la segunda zona Z2 y es por consiguiente inútil conservar una copia dentro de la primera zona Z1.

El sistema de explotación de confianza 30 procede entonces en la etapa E14 a la elaboración de una lista de partición L2 que comprende por ejemplo para cada archivo cargado en la segunda zona Z2, como se ha representado en la figura 6:

- una designación DES del archivo en cuestión;
- la dirección (aquí virtual) ADR de memorización del archivo en cuestión, tal como se utiliza por el sistema de explotación polivalente 20 para acceder al archivo (o sea una dirección comprendida en el tercer margen P3 de direcciones);
- informaciones INT de comprobación de la integridad del archivo en cuestión, por ejemplo en forma de un código de control por redundancia cíclica (o CRC por "*cyclic redundancy check*");
- un certificado CERT generado para el archivo en cuestión por el sistema de explotación de confianza 30 (con el fin de permitir ulteriormente al sistema de explotación polivalente 20 comprobar que el sistema de explotación de confianza 30 se encuentra en el origen de carga del archivo en cuestión en la segunda zona Z2)

En el ejemplo descrito aquí, las informaciones de comprobación INT se obtienen como se ha indicado anteriormente por aplicación de un algoritmo de control de redundancia cíclica en los márgenes de memoria donde se memoriza el archivo en cuestión. Se utiliza por ejemplo uno de los algoritmos siguientes: SHA-2, SHA-3 (SHA procedente del inglés "*Secure Hash Algorithm*") o MD5 (del inglés "*Message-Digest*" 5). En variante, se podría utilizar una suma de control (en inglés "*checksum") o un código de autentificación (o MAC, del inglés "*Message Authentication Code*").*

La lista de partición L2 puede eventualmente contener además, para cada archivo cargado en la segunda zona Z2, la dirección física de memorización del archivo en la memoria de acceso aleatorio 4.

El sistema de explotación de confianza 30 transmite en la etapa E16 la lista de partición L2 así elaborada al sistema de explotación polivalente 20. Como anteriormente, esta transmisión es aquí realizada por mediación del monitor de seguridad 40 con conmutación al entorno de ejecución polivalente REE.

En variante, la lista de partición L2 podría ser memorizada por el sistema de explotación de confianza 30 en un emplazamiento predefinido de memoria accesible por el sistema de explotación polivalente 20, por ejemplo en un emplazamiento predefinido de la segunda zona Z2 de memoria de acceso aleatorio 4.

Con el fin de comprobar que la lista de partición L2 no está corrompida cuando se utiliza, se puede memorizar un código de redundancia cíclica (o CRC) generado por el sistema de explotación de confianza 30 y asociado con la lista de partición L2.

Debido a la conmutación iniciada en la etapa E16, el sistema de explotación polivalente 20 es de nuevo ejecutado en la etapa E18 y memoriza la lista de partición L2 recibida (o tiene acceso a la lista de partición L2 en el emplazamiento predefinido en la variante que acaba de ser mencionada), con comprobación eventual del código de redundancia cíclica asociado con la lista de partición L2.

Durante el funcionamiento ulterior del aparato electrónico 10, el sistema de explotación polivalente 20 y las aplicaciones ejecutadas dentro del marco del entorno de ejecución polivalente REE podrán así consultar la tabla de partición L2 y acceder a los archivos memorizados en la segunda zona Z2 en la dirección ADR indicada en la tabla de partición L2 para el archivo en cuestión, comprobando eventualmente la integridad del archivo gracias a las informaciones INT presentes en la tabla de partición L2 para el archivo en cuestión y/o el origen del archivo gracias al certificado CERT presente en la tabla de partición L2 para el archivo en cuestión.

Sobre la base de la lista de partición L2 recibida (o consultable en el emplazamiento predefinido) y de la lista de requisitos L1 preparada en la etapa E7, el sistema de explotación polivalente 20 determina (por diferencia) en la etapa E20 que archivos referenciados en la lista de requisitos L1 no han sido cargados en la segunda zona Z2 (estando los archivos cargados en la segunda zona Z2 designados en la lista de partición L2).

Los archivos determinados en la etapa E20 como presentes en la lista de requisitos L1 y ausentes de la lista de partición L2 son entonces cargados en la etapa E22 en la tercera zona Z3, es decir copiados de la memoria no-volátil reprogramable 6 (donde han sido previamente instalados) a la tercera zona Z3 de la memoria de acceso aleatorio 4 bajo el control del sistema de explotación polivalente 20.

La memorización correcta de los archivos en la tercera zona Z3 es por otro lado eventualmente comprobada por el sistema de explotación polivalente 20, por ejemplo por la espera de un indicador de buen funcionamiento procedente de la memoria de acceso aleatorio 4 (eventualmente acompañado de una suma de control de los datos escritos en la memoria) y/o lectura de los datos escritos para comparación con los datos a escribir.

La carga de los archivos en las diferentes zonas Z1, Z2, Z3 de la memoria de acceso aleatorio 4 ha terminado así y el funcionamiento normal puede por consiguiente empezar en la etapa E24, por ejemplo por la espera de un comando del usuario a nivel de la interfaz hombre máquina (no representada) del aparato electrónico 10.

El funcionamiento normal se continúa hasta el momento en que una nueva aplicación es instalada dentro del marco del funcionamiento en el entorno de ejecución polivalente REE.

El sistema de explotación polivalente 20 prepara entonces una lista de requisitos actualizada L1' y transmite esta lista de requisitos al sistema de explotación de confianza 30 en la etapa E26.

El sistema de explotación de confianza 30 recibe la lista de requisitos actualizada L1' y determina (como en la etapa E10) los nuevos archivos a cargar en la segunda zona Z2, así como eventualmente los archivos a eliminar de la segunda zona Z2 con el fin de liberar espacio de memoria para los nuevos archivos. Se utiliza por ejemplo en este marco un método de gestión de páginas de memoria de tipo FIFO (del inglés "*First In, First Out*"), o LRU (del inglés "*Least Recently Used*", o LFU (del inglés "*Least Frequently Used*"), o también del tipo prioridad aleatoria (o "*Random Priority*").

El sistema de explotación de confianza 30 calcula entonces un código de redundancia cíclico relacionado con los nuevos archivos a cargar en la segunda zona Z2 y comanda la escritura de los nuevos archivos en la segunda zona Z2 (etapa E30).

El sistema de explotación de confianza 30 actualiza entonces en la etapa E32 la lista de partición L2 (para tener en cuenta los nuevos archivos cargados en la segunda zona Z2). El procedimiento continua entonces en la etapa E16 descrita a continuación para conmutación hacia el entorno de ejecución polivalente REE con envío de la lista de partición (actualizada) y carga en la zona Z3 de los archivos necesarios para el funcionamiento de la nueva aplicación y que no han sido cargados en la zona Z2.

En variante a las etapas E26 a E32 que acaban de describirse, el procedimiento podría concluir en la etapa E4 en la instalación de una nueva aplicación en el entorno de ejecución polivalente REE con el fin de llevar a cabo en su totalidad el procedimiento de carga de archivos en la zona Z2 tal como se ha descrito anteriormente en las etapas E4 a E16.

REIVINDICACIONES

1. Procedimiento de carga de aplicación en memoria de acceso aleatorio (4) en un aparato electrónico (10) concebido para funcionar en un entorno de ejecución de confianza (TEE), debido a la ejecución de un sistema de explotación de confianza (30) por un procesador (2) del aparato electrónico (10), o en un entorno de ejecución polivalente (REE), caracterizado por que comprende las etapas siguientes:

- recepción (E10), por el sistema de explotación de confianza (30), de informaciones (L1) que identifican al menos una aplicación, estando las informaciones que identifican la mencionada aplicación contenidas en un descriptivo de requisitos (L1) preparado durante el funcionamiento en el entorno de ejecución polivalente (REE);

- comprobación (E11), por el sistema de explotación de confianza (30), de la conformidad de la aplicación identificada con al menos un criterio dado;

- en caso de conformidad, carga (E13) de la aplicación identificada en una zona (Z2) de memoria de acceso aleatorio (4) accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente (REE).

2. Procedimiento de carga según la reivindicación 1, en el cual el descriptivo de requisitos (L1) es elaborado (E7) en función de los datos (T1) representativos de las frecuencias de utilización de las aplicaciones instaladas en el entorno de ejecución polivalente (REE).

3. Procedimiento de carga según la reivindicación 1 o 2, en el cual el descriptivo de requisitos (L1) es elaborado (E7) en función de las estadísticas de utilización relacionadas con varios criterios.

4. Procedimiento de carga según una de las reivindicaciones 1 a 3, que comprende las etapas siguientes, ejecutadas en el entorno de ejecución polivalente (REE) para cada aplicación mencionada en el descriptivo de requisitos (L1):

- determinación si la aplicación mencionada está cargada en la indicada zona (Z2) de memoria de acceso aleatorio (4) accesible solo en lectura;

- en caso negativo, carga de la aplicación en cuestión en otra zona (Z3) de la memoria de acceso aleatorio (4) accesible en escritura durante el funcionamiento en el entorno de ejecución polivalente (REE).

5. Procedimiento de carga según una de las reivindicaciones 1 a 4 que comprende una etapa de construcción (E14), por el sistema de explotación de confianza (30), de una lista de partición (L2) que incluye una designación (DES) de la aplicación cargada y una dirección (ADR) de memorización de la aplicación cargada.

6. Procedimiento de carga según la reivindicación 5, en el cual la lista de partición (L2) incluye una información (INT) de comprobación de integridad asociada con la aplicación cargada.

7. Procedimiento de carga según la reivindicación 5 o 6, en el cual la lista de partición (L2) incluye un certificado (CERT) generado por el sistema de explotación de confianza (30) y relacionado con la aplicación cargada.

8. Procedimiento de carga según una de las reivindicaciones 5 a 7, en el cual la lista de partición (L2) se memoriza en la indicada zona (Z2) de memoria de acceso aleatorio (4) accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente (REE).

9. Procedimiento de carga según una de las reivindicaciones 1 a 8, en el cual la mencionada carga se realiza a partir de una memoria no volátil (6).

10. Procedimiento de carga según una de las reivindicaciones 1 a 9, en el cual la indicada zona (Z2) es accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente (REE) por medio de direcciones virtuales apuntando a direcciones físicas distintas de las direcciones virtuales en cuestión.

11. Procedimiento de carga según una de las reivindicaciones 1 a 10, en el cual las informaciones (L1) que identifican la aplicación son recibidas durante una conmutación del entorno de ejecución polivalente (REE) al entorno de ejecución de confianza (TEE).

12. Procedimiento de carga según una de las reivindicaciones 1 a 11, que comprende además las etapas siguientes:

- a continuación de una instalación de una nueva aplicación en el entorno de ejecución polivalente (REE), transmisión (E26) al sistema de explotación de confianza (30) de un descriptivo de requisitos actualizado (L1');

- carga (E30), en la zona (Z2) de memoria de acceso aleatorio (4) accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente (REE), de un nuevo archivo designado en el descriptivo de requisitos actualizado (L1').

13. Aparato electrónico (10) que comprende al menos un procesador (2) y una memoria de acceso aleatorio (4) y concebido para funcionar en un entorno de ejecución de confianza (TEE), debido a la ejecución de un sistema de explotación de confianza (30) por el procesador (2), o en un entorno de ejecución polivalente (REE), caracterizado por que el sistema de explotación de confianza (30) está concebido para recibir informaciones (L1) que identifican al menos una aplicación, estando las informaciones que identifican la mencionada aplicación contenidas en un descriptivo de requisitos (L1) preparado durante el funcionamiento en el entorno de ejecución polivalente (REE), para comprobar la conformidad de la aplicación identificada con al menos un criterio dado y para cargar, en caso de conformidad, la aplicación identificada en una zona (Z2) de la memoria de acceso aleatorio (4) accesible en lectura solo durante el funcionamiento en el entorno de ejecución polivalente (REE).

Fig.1

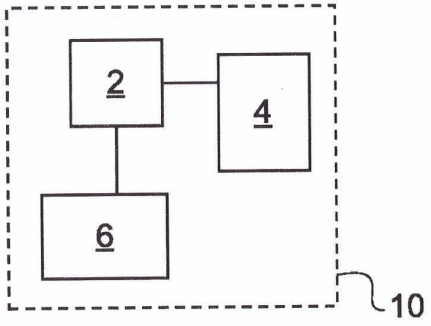


Fig.2

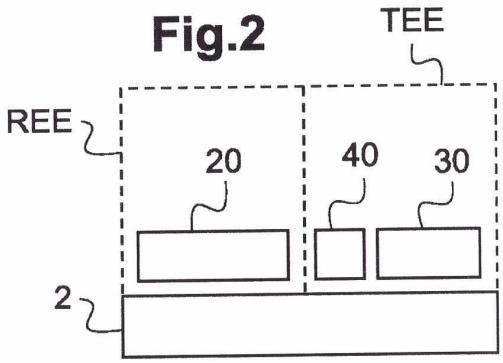
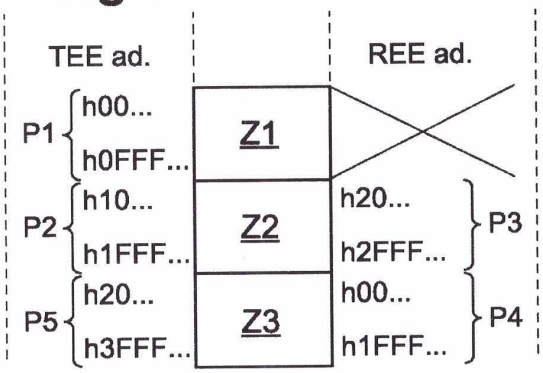


Fig.3



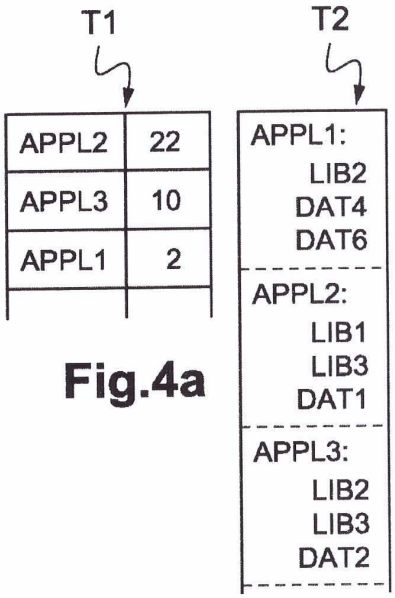


Fig.4a

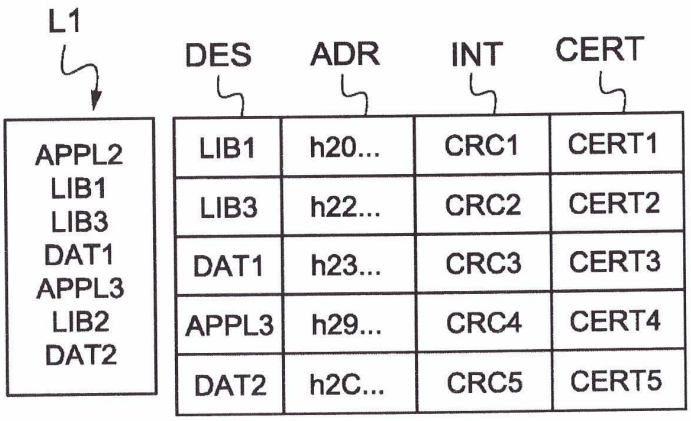


Fig.6

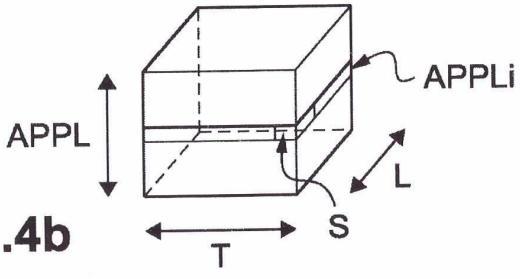
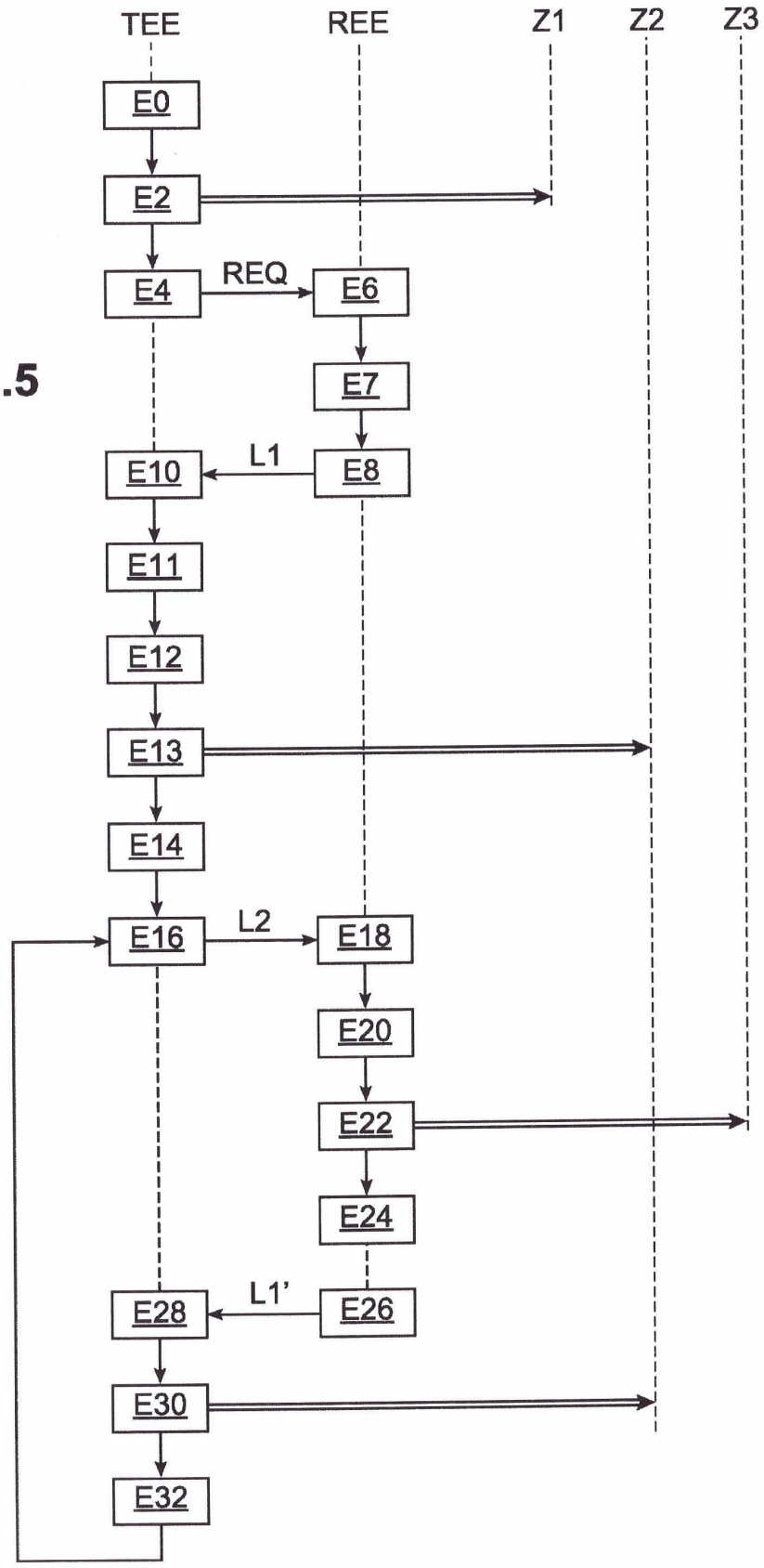


Fig.4b

Fig.5


TEE
REE
Z1
Z2
Z3
E0
E2
E4
REQ
E6
E7
E10
L1
E8
E11
E12
E13
E14
E16
L2
E18
E20
E22
E24
E28
L1'
E26
E30
E32