(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 336 356**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06300043 .4**
(96) Fecha de presentación : **19.01.2006**
(97) Número de publicación de la solicitud: **1688818**
(97) Fecha de publicación de la solicitud: **09.08.2006**

(54) Título: **Procedimiento para gestionar de manera segura la ejecución de una aplicación.**

(30) Prioridad: **04.02.2005 FR 05 50323**

(45) Fecha de publicación de la mención BOPI:
12.04.2010

(45) Fecha de la publicación del folleto de la patente:
12.04.2010

(73) Titular/es: **Société Française du Radiotéléphone**
Tour Séquoia - La Defénse 6
1, place Carpeaux
92915 Paris La Défense Cédex, FR

(72) Inventor/es: **Hybre, Jean y**
Wary Jean-Philippe

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento para gestionar de manera segura la ejecución de una aplicación.

La presente invención tiene por objeto un procedimiento para gestionar de manera segura la ejecución de una aplicación. El dominio de la invención es el de la telefonía móvil y más particularmente de los terminales inteligentes conectados a las redes de telefonía móvil. Un terminal llamado "inteligente" a lo largo del texto es un teléfono móvil apto para telecargar contenidos multimedia o activos. Un contenido activo es un programa que puede ejecutarse sobre un teléfono móvil y por consiguiente poner en práctica las funcionalidades del citado teléfono móvil. Se considera aquí que todos los teléfonos a los que se hace referencia son terminales inteligentes. Un teléfono inteligente permite gestionar diferentes recursos internos, siendo estos recursos accesibles desde diferentes puertos de extensión o contenidos telecargados o activos. La presente definición no es limitativa de la invención.

Un objeto de la invención es hacer seguro el acceso a los recursos del teléfono móvil por los programas que se ejecutan en el citado teléfono móvil.

En la técnica más avanzada se conocen entornos de ejecución de código seguros. Estos entornos están basados sobre la puesta en práctica de una "máquina virtual" que es una sobrecapa de un sistema de explotación del teléfono móvil. Esta máquina virtual ejecuta programas específicamente escritos para ella. La máquina virtual es por consiguiente necesaria para la puesta en práctica de estos programas. La máquina virtual es un intermedio entre el programa específico y el sistema de explotación del teléfono móvil, por consiguiente entre el programa específico y las funcionalidades del teléfono móvil.

Por consiguiente, por una parte el hecho de que un teléfono contenga una máquina virtual no impide la puesta en práctica de otros programas no específicos que acceden a las funcionalidades del teléfono móvil. Una política de seguridad puesta en práctica por la máquina virtual está por consiguiente definida para los programas específicos.

Por otra parte tales políticas siguen estando confinadas al nivel del teléfono móvil, sin interacción prevista con la tarjeta SIM por ejemplo. Tal modelo de seguridad es por ejemplo el modelo MIDP 2.0 correspondiente al lenguaje y a la máquina virtual Java.

El documento XP 002341584 C "Computer Security Basics" (O'Reilly, Rusell & Gangemi) describe un control de acceso a ficheros en un ordenador.

En la técnica más avanzada se conocen también políticas de seguridad gestionadas por dominio, perteneciendo cada aplicación a un dominio. Un dominio define los derechos de acceso a funcionalidades definidos de manera precisa, incluso a la totalidad de las funcionalidades del teléfono. En este caso cualquier aplicación debe pertenecer a un dominio. Así, si una aplicación tiene necesidad de derechos específicos es preciso definir y asignarle un nuevo dominio, es decir redefinir los derechos para todas las funcionalidades del teléfono móvil en el cual se ejecuta la aplicación, incluyendo para las funcionalidades que la aplicación no utiliza.

En la gestión de derechos por dominio, la puesta en práctica de los derechos se hace por dominio, es decir para todas las aplicaciones que pertenecen al citado dominio. Actualizar derechos para una aplicación específica independientemente de otras aplicaciones es por consiguiente imposible.

En la invención se resuelven estos problemas asociando a cada aplicación un identificador. Cuando una aplicación está activa, una ocurrencia de ésta es gestionada por el sistema de explotación del teléfono. Esta gestión se realiza generalmente a través de un contexto de memoria descriptivo del estado actual de esta ocurrencia de aplicación, de los recursos consumidos, de los sistemas de comunicaciones utilizados, de los procesos padres e hijos ligados a la aplicación en un instante dado (la lista es no exhaustiva y no es limitativa de la invención). Este contexto es el punto de entrada del sistema de explotación para gestionar las prioridades y las interrupciones entre o *inter* aplicaciones. En el marco de la invención, el identificador de la aplicación es un dato cuyo valor es una constante, dato registrado en el contexto de memoria gestionado por el sistema de explotación para la ocurrencia actual de la aplicación activa. En el caso de que varias ocurrencias de la aplicación estén activas al mismo tiempo, el sistema de explotación gestiona varios contextos de memoria diferentes, pero el valor del identificador de aplicación tiene entonces el mismo valor para el conjunto de los contextos puesto que estamos frente al mismo código aplicativo.

En la invención cada recurso está claramente identificado y es identificable como recurso cuando una aplicación busca acceder a él. Esta identificación del recurso puede ser implícita puesto que en este caso se realiza a través del uso de una interfaz de programa (API) claramente identificada o puede ser explícita durante el uso de una dirección de memoria identificada a su vez como un recurso que se desea proteger. Una definición más exhaustiva de la noción de recurso se proporciona más adelante. En la invención cada recurso está asociado a una tabla de identificadores de aplicaciones, estando cada identificador de esta lista asociado a un derecho relativo al recurso. Cuando la aplicación busca acceder a un recurso o funcionalidad del teléfono móvil, el sistema de explotación recorre la tabla asociada al recurso para determinar si la aplicación está identificada y extraer los derechos que posee la aplicación con respecto al recurso. El desarrollo de la ejecución de la aplicación está condicionado por la lectura de estos derechos.

En la invención cada recurso está asociado a un propietario solo habilitado para modificar la tabla asociada al recurso.

En la invención es por consiguiente posible definir de manera fina los derechos asociados a una aplicación y hacerlos evolucionar sin afectar a las otras aplicaciones.

La invención tiene por consiguiente por objeto un procedimiento para gestionar de manera segura la ejecución de aplicaciones en un teléfono móvil, accediendo una aplicación a recursos del teléfono móvil gestionados mediante un sistema de explotación caracterizado porque un recurso del teléfono móvil es identificable y está asociado a una tabla de identificadores de aplicaciones permitidas o no que puede poner en práctica el recurso, teniendo el recurso un propietario solo autorizado a actualizar la lista de aplicaciones, aplicando el sistema de explotación para cada recurso al que se accede los derechos correspondientes a la aplicación que accede, comprendiendo cada aplicación un identificador único.

Ventajosamente la invención está también caracterizada porque el sistema de explotación gestiona una tabla dinámica y temporal por identificador de aplicación que permite mantener las autorizaciones de uso de los recursos ya autorizados para cada una de las aplicaciones.

Ventajosamente la invención está también caracterizada porque el sistema de explotación libera las autorizaciones de acceso a un recurso para la aplicación identificada al final del tiempo asignado, o a la salida de un espacio geográfico predeterminado.

Ventajosamente la invención está también caracterizada porque los recursos del sistema de explotación comprenden memorias y/o zonas de memorias del teléfono móvil.

Ventajosamente la invención está también caracterizada porque los recursos del sistema de explotación comprenden medios de comunicaciones para el teléfono móvil.

Ventajosamente la invención está también caracterizada porque los propietarios de los recursos están al menos en una lista compuesta por usuarios del teléfono, del operador de telefonía móvil, del constructor del teléfono móvil y de suministradores del contenido.

Ventajosamente la invención está también caracterizada porque el acceso a los recursos está centralizado al nivel de una interfaz de programa (API), permitiendo esta interfaz el acceso a un recurso si la aplicación que busca acceder a este recurso posee los derechos requeridos.

Ventajosamente la invención está también caracterizada porque cada tabla de identificadores de aplicaciones asociada a un recurso comprende un identificador correspondiente a las aplicaciones no listadas en la tabla para definir los derechos por defecto de una aplicación.

Ventajosamente la invención está también caracterizada porque pueden definirse derechos por defecto para los accesos a los recursos de un mismo propietario, pudiendo realizarse esta definición por ejemplo durante la configuración del móvil a la salida de fabricación.

Ventajosamente la invención está también caracterizada porque una tabla de identificadores que comprende entradas correspondientes a certificados electrónicos permite agrupar bajo un mismo propietario a varias familias de certificados electrónicos.

Ventajosamente la invención está también caracterizada porque un acceso a un recurso está comprendido en el conjunto que comprende al menos los elementos siguientes: lectura, escritura, modificación, destrucción, ejecución de datos o de código ejecutable.

Ventajosamente la invención está también caracterizada porque, cuando se descuelga el teléfono un programa de descuelgue verifica la integridad de las tablas de identificadores y de la parte del sistema de explotación que accede a estas tablas de identificadores.

Ventajosamente la invención está también caracterizada porque cuando se descuelga el teléfono un programa de descuelgue verifica la integridad de las partes del sistema de explotación a cargo de las funciones de control y de seguridad del teléfono, permitiendo estos controles cuando se descuelga el teléfono garantizar que sólo y exclusivamente el sistema de explotación original del constructor está instalado en el teléfono y es utilizado por éste.

Ventajosamente la invención está también caracterizada porque un derecho de acceso a un recurso está comprendido en el conjunto que comprende al menos los elementos siguientes: acceso autorizado, acceso autorizado una vez, acceso autorizado N veces, siendo N parametrizable, acceso denegado, solicitar la autorización al usuario una vez, solicitar la autorización al usuario para cada acceso, solicitar la autorización al usuario para N accesos, siendo N parametrizable, solicitar la asignación de un código una vez, solicitar la asignación de un código para cada acceso, solicitar la asignación de un código para N accesos, siendo N parametrizable, solicitar un cálculo o un enigma criptográfico

para autorizar el acceso una vez, solicitar un cálculo o un enigma criptográfico para autorizar cada acceso, solicitar un cálculo o un enigma criptográfico para autorizar N accesos, siendo N parametrizable.

Ventajosamente la invención está también caracterizada porque la tabla de identificadores de aplicaciones tiene un tamaño dinámico.

Ventajosamente la invención está también caracterizada porque cada nueva aplicación es analizada para actualizar las tablas de identificadores de aplicaciones.

Un modo de realización de la invención se describe en la reivindicación 1, así como modos alternativos en las reivindicaciones dependientes.

La invención se comprenderá mejor con la lectura de la descripción que sigue y con el examen de las figuras que la acompañan. Éstas se presentan a título indicativo y en absoluto limitativo de la invención. Las figuras muestran:

Figura 1: una ilustración de medios que permiten la puesta en práctica del procedimiento de acuerdo con la invención.

Figura 2: una ilustración de etapas del procedimiento de acuerdo con la invención.

La figura 1 muestra un teléfono 101 móvil conectado a una red 102 de telefonía móvil por medio de una antena 103 conectada a circuitos 104 de interfaz entre la red 102 y un bus 105 interno del teléfono 101.

El teléfono 101 comprende también en particular pero de manera no limitativa, un microprocesador 106, una pantalla 107, una memoria 108 de programa, una memoria 109 de descuelgue y una memoria 110 de tablas de identificadores. Los elementos 106 a 110 están interconectados por el bus 105. El teléfono 101 comprende otros órganos no representados como un teclado, un micrófono,... la lista no es exhaustiva.

Cuando se presta una acción a un aparato ésta se realiza de hecho mediante un microprocesador de este aparato accionado mediante códigos de instrucciones registrados en una memoria de programa del citado aparato. Se presta también una acción a una aplicación. Esto significa que una parte de los códigos de instrucciones que constituyen la aplicación es ejecutada por el microprocesador.

La memoria 109 comprende códigos de instrucciones ejecutados por el microprocesador 106 cuando se proporciona tensión al teléfono 101. En la práctica se trata de una ROM o de una PROM, lo que hace la corrupción de los códigos de instrucciones que están registrados en ella muy difícil y reservada a especialistas.

La memoria 108 es la memoria de programa del teléfono 101. Para comprender mejor la invención se ha dividido la memoria 108 en 3 zonas. Una zona 108a de recursos, una zona 108b de sistema de explotación y más particularmente de gestión del acceso a los recursos, y una zona 108c de aplicaciones utilizables por un usuario del teléfono 101. La zona 108a corresponde lo que se llama comúnmente el “firmware” y comprende los pilotos de acceso a los recursos materiales.

Un recurso es aquí un concepto general. Se trata en la práctica de un recurso material, de una funcionalidad del teléfono 101 ó de uno o varios objetos.

El recurso material puede ser una zona de memoria del teléfono 101, estando esta zona en el teléfono, en un componente amovible de almacenamiento o de extensión de las funcionalidades del teléfono, o en una tarjeta SIM/USIM conectada al teléfono 101. En el caso de un contenido de multimedia almacenado en el teléfono, el recurso puede ser definido como la zona de almacenamiento de estos contenidos de multimedia o como varias zonas, correspondiendo cada una a un contenido único. Un recurso puede describirse también como un intervalo de direcciones sobre un bus.

Un recurso puede verse igualmente como una función. Tales funciones son por ejemplo leer o escribir una zona de memoria, leer o escribir sobre un puerto de extensión (Infrarrojo, Bluetooth, conexión de serie, no siendo la lista limitativa ...), utilizar las funcionalidades de un coprocesador o de un componente activo a través de un intervalo de dirección de memoria o de una interfaz de programa (API), leer, escribir, enviar o recibir un SMS, un MMS, un mensaje, un correo electrónico, leer el IMEI del teléfono, leer el identificador del teléfono de célula de estación de base a la cual está conectado el teléfono, leer la localización geográfica del teléfono cualquiera que sea el sistema de adquisición de coordenadas geográficas utilizado (por ejemplo a través de una interfaz de programa con un sistema de GPS), leer o escribir en el anuario del teléfono (correspondiendo el anuario de hecho a una zona de memoria), mostrar o borrar un objeto en la pantalla, enviar una orden hacia la tarjeta SIM/USIM, ..., la lista no es exhaustiva.

Un recurso puede también corresponder a uno o a varios objetos diferentes (anuario, entrada en un anuario, datos del calendario, uno o varios juegos, un trozo de música, una película,..., esta lista no es limitativa de la invención).

Los recursos pueden constituir también lo que se puede llamar una interfaz de programa: Una interfaz de programa es un conjunto de funciones que pueden ser puestas en práctica mediante una aplicación. En nuestro ejemplo una interfaz centralizada agrupa a todas las funciones que permiten el acceso a los recursos del teléfono. No existe otro medio para una aplicación de acceder a un recurso que poner en práctica una función de la interfaz centralizada.

La zona 108 corresponde al sistema de explotación que comprende la mayoría del tiempo la zona 108a. Aquí lo hemos separado para poner en evidencia el hecho de que el sistema de explotación comprende un módulo 111 de verificación de los derechos de acceso a los recursos.

La zona 108c comprende los códigos de instrucciones de las aplicaciones instaladas en el teléfono 101. Una aplicación es, por ejemplo, una agenda, una calculadora, un cliente de mensajería (SMS, MMS, correo electrónico u otro), juegos, visualizadores de mono o multimedia,... la lista no es exhaustiva. Cada aplicación está identificada mediante un identificador de aplicación.

El modo de representación de la memoria 108 ilustra el hecho de que una aplicación que busca acceder a un recurso del teléfono móvil lo hace a través del sistema de explotación, por consiguiente a través del módulo 111 de verificación de los derechos de acceso a los recursos. Cada recurso está identificado mediante un identificador de recurso.

La memoria 110 está subdividida en registros 112.1 a 112.N, siendo cada registro identificado por un identificador 113 de recurso. Un registro comprende también una tabla 114 que asocia identificadores 114a de aplicaciones a derechos 114b. Derechos son por ejemplo lectura, escritura, acceso sometido a la petición de autorización, acceso sometido a la asignación de un código.

La tabla 114, por consiguiente el registro 112, es de tamaño variable en función del número de identificadores de aplicaciones que contiene. Tal tabla se aumenta cuando es necesario. Esto permite una gestión eficaz de la memoria del teléfono móvil. En efecto para la inscripción de un nuevo derecho, si la tabla es demasiado pequeña, entonces aumenta dinámicamente.

Un registro de la memoria 114 comprende también un campo 116 que comprende derechos por defecto. Estos derechos son aplicados cuando una aplicación que busca acceder al recurso no está descrita por un identificador específico en el registro de la memoria 110 correspondiente al recurso.

En una variante de la invención un registro 112 comprende también un identificador 115 de propietario. Un identificador de propietario es bien una palabra alfanumérica arbitraria, bien una firma digital del contenido de un recurso o de una aplicación, mediante un certificado. La firma así obtenida está asociada a la parte pública de certificado que tiene permiso para obtener la firma. Es así posible verificar la firma y confirmar mediante la misma la identidad del propietario.

La figura 2 muestra una etapa 201 preliminar en la cual un usuario del teléfono 101 lo pone en tensión. El microprocesador ejecuta entonces los códigos de instrucciones registrados en la memoria 109. En una variante de la invención los códigos de instrucciones de la memoria 109 permiten validar el módulo 111 y la memoria 110, efectuando una suma de control por ejemplo o una validación criptográfica de la integridad con prueba de origen del código, permitiendo establecer que el constructor del teléfono está en el origen de la puesta en práctica de los módulos 111 y de la memoria 110... Esto permite garantizar que la política de acceso a los recursos del teléfono 101 no ha sido alterada.

De la etapa 201, se pasa a etapas de utilización del teléfono 101 entre las cuales se encuentra una etapa 202 de lanzamiento de una aplicación. Por ejemplo el lanzamiento de una aplicación de consulta de un anuario que comprende el teléfono 101. En la práctica, tal anuario corresponde a una zona de una memoria del teléfono 101.

Una vez que la aplicación está lanzada va a tratar de acceder, en una etapa 201 a uno o a varios recursos del teléfono 101. Cuando una aplicación busca acceder a un recurso, esta tentativa de acceso es interceptada por el módulo 111. En el momento de la interceptación del módulo 111 está en conocimiento de la aplicación, por medio de su identificador idAP, y del recurso, por medio de su identificador idR, al cual la citada aplicación busca acceder.

En la etapa 203 el módulo 111 efectúa entonces varias acciones. En una etapa 204 el módulo 111 busca en la memoria 110 el registro correspondiente al identificador idR. Una vez encontrado este registro, por ejemplo 112.1, se pasa a una etapa 205 de búsqueda de la aplicación correspondiente al identificador idP en la tabla 114 del registro 112.1.

Si está búsqueda 205 tiene éxito, se pasa a una etapa 206, si no se pasa a una etapa 207.

La etapa 205 consiste en un recorrido secuencial de la tabla 114 hasta encontrar una línea cuyo contenido de la columna 114a corresponde al identificador idAp, o hasta el final de la tabla 114. Esto permite determinar una línea en la tabla 114, o respectivamente concluir en la no presencia del identificador idAp en la tabla 114.

En la etapa 206 el módulo 111 lee el contenido de la columna 114b correspondiente a la línea determinada en la etapa 205. Se trata de una etapa de lectura de derecho. De la etapa 206 se pasa entonces a una etapa 210 de aplicación del derecho.

En la etapa 207 el módulo 111 busca leer un certificado de identificación ligado a la aplicación. Este certificado está registrado en la aplicación de la misma manera que el identificador de aplicación. Si tal certificado existe se pasa a una etapa 208, si no se pasa a una etapa 209.

En la etapa 208 el módulo 111 comienza por verificar la validez del certificado. Con este fin el móvil comprende un cierto número de certificados pre-registrados, por ejemplo un certificado de operador en la tarjeta SIM, un certificado de constructor en el código de descuelgue y un certificado de suministrador de contenidos en el móvil o la tarjeta SIM. El certificado de aplicación, para ser válido debe ser compatible con uno de los certificados conocidos por el teléfono 101. Esta compatibilidad es verificada, por ejemplo, mediante el cifrado de un riesgo a partir de una clave del certificado de la aplicación, debiendo uno de los certificados conocidos por el teléfono móvil permitir recuperar este riesgo.

En una variante la aplicación comprende también una firma ligada al certificado que presenta. Esta firma es una firma electrónica realizada sobre la base de la clave privada del certificado y del contenido de la aplicación, es decir de los códigos de instrucciones que la componen. La verificación se efectúa por consiguiente de manera clásica a partir de la clave pública del certificado y del contenido de la aplicación.

Si el certificado es válido, entonces el módulo 111 recorre la tabla 114 a la búsqueda del certificado de aplicación, lo que permite, como para un certificado de aplicación, determinar una línea en la tabla 114, y por consiguiente leer derechos. En esta variante de registro 112.x comprende por consiguiente una tabla que asocia certificados a derechos de acceso al recurso identificado por el contenido del campo 113. Esta asociación se realiza a través de una firma del contenido de la aplicación mediante el certificado.

Si el certificado es válido, la etapa 208 es seguida de una etapa 210, si no es seguida de la etapa 209.

El módulo 111 desemboca en la etapa 209 si ha sido imposible identificar la aplicación por cualquier medio. En este caso los derechos aplicados serán derechos por defecto, correspondiendo éstos al contenido del campo 116.

En una variante de la invención, los derechos por defecto son definidos en función del propietario del recurso. Si el campo 116 no está registrado para un recurso al cual desea acceder una aplicación, entonces existe una tabla 118 registrada en una memoria conectada al bus 105 y que asocia derechos por defecto a un propietario. Los derechos que se van a aplicar son entonces buscar en esta tabla 118 en función del identificador 115 de propietario del recurso al que se debe acceder. Esta tabla es, por ejemplo, registrada en el momento de la fabricación del teléfono. Por consiguiente puede ser también actualizada.

La determinación de los derechos por defecto puede también, en una variante, ser realizada sobre la base de un certificado ligado a la aplicación o a un propietario de la aplicación. En este caso una aplicación comprende un certificado o un identificador de propietario. Una memoria 119 del teléfono 101, conectada al bus 105, comprende entonces una tabla que asocia un certificado, y/o un propietario, a derechos por defecto.

En una variante de la invención la memoria 119, o en otra memoria no descrita, permite asociar varios certificados a un certificado llamado maestro. Este certificado maestro corresponde a un propietario y por consiguiente a derechos asociados. En particular el propietario así identificado por medio del certificado maestro puede modificar los derechos asociados a los certificados a su vez asociados al certificado maestro.

De la etapa 209 se pasa a la etapa 210.

En la etapa 210, el módulo 111 responde a la aplicación que haya solicitado el acceso a un recurso en función de los derechos leídos en una de las etapas 206, 208 ó 209.

Esta respuesta es por consiguiente por ejemplo, acceso autorizado, acceso denegado, solicitar la autorización al usuario, solicitar la asignación de un código, solicitar un enigma criptográfico.

De manera fina el acceso puede ser autorizado en lectura, escritura, modificación, destrucción, ejecución.

La solicitud de autorización al usuario se traduce en un mensaje visualizado sobre la pantalla 107. Este mensaje es del tipo “la aplicación Ap desea acceder a R. Autorizar: ¿sí/no?”.

La solicitud de código para el usuario se traduce en un mensaje visualizado en la pantalla 107. Este mensaje es del tipo “la aplicación Ap desea acceder a R. Asignar código:”.

En el caso de un enigma criptográfico, no hay solicitud de autorización del usuario, gestionando el propio teléfono la autorización de acceso de la aplicación si las respuestas a los enigmas criptográficos están de acuerdo con las esperadas del módulo 111.

Las respuestas a estos mensajes determinan el resultado de la ejecución de la aplicación. En otros términos, si las respuestas a estas preguntas son sí, el código correcto o los enigmas criptográficos son válidos, entonces el acceso es autorizado, si no el acceso es denegado.

En una variante de la invención, la aplicación puede ser autorizada para un número N, parametrizable, de accesos.

De la etapa 203 se pasa a una etapa 211 de desarrollo de la ejecución de la aplicación. En esta etapa la aplicación recibe la respuesta del módulo 111 con respecto a su solicitud de acceso a un recurso. Si la respuesta es positiva entonces la ejecución se lleva a cabo normalmente, si no la ejecución es interrumpida.

En una variante de la invención el componente 111 guarda y mantiene un contexto relativo a la autorización acordada para la citada aplicación o solicitud de aplicación de acceso al recurso de manera que aumenten los rendimientos del sistema para no tener que probar de nuevo permanentemente los derechos de acceso a los recursos. Existe por consiguiente una gestión de una tabla 117 registrada en una memoria conectada con el bus 105, temporal y dinámica de autorización clasificada por idAP y que contiene los recursos autorizados, o clasificada por idAP y el identificador de la instancia en el caso en el que la aplicación se ejecute varias veces. La tabla 117 es por ejemplo una memoria temporal que conserva los resultados de las interrogaciones hechas en la etapa 203. Ya no es por consiguiente útil acceder a la memoria 110 para obtener la respuesta a una interrogación que ya ha sido tratada. En otro ejemplo la memoria 110 es una copia de una parte de la memoria 110, correspondiendo la citada parte a porciones de tablas de identificadores de aplicación, siendo estas porciones de tablas las que ya han sido revisadas.

En otra variante los derechos de acceso al recurso son también memorizados en la tabla temporal y liberados cuando se libera el recurso.

En otra variante más, las autorizaciones de acceso pueden ser asignadas para una duración de uso predeterminada y liberadas cuando se libera el recurso o al finalizar la duración del uso asignada, pudiendo ser la definición de esta duración global para todos los recursos del móvil, específica por aplicación, específica por recurso al que se accede. Pudiendo el cálculo del tiempo de uso del recurso o de los recursos ser realizado con la puesta en práctica de un contador de tiempo, de manera atómica por recurso, o de manera global por aplicación para un conjunto de recursos, por recurso para un conjunto de aplicaciones o para un conjunto de aplicaciones para un conjunto de recursos. En esta variante, por ejemplo, se utiliza la tabla 117 asociando a cada resultado de interrogación una condición de validez ya sea temporal, en número de interrogaciones, o geográfica. Cuando la condición de validez expira, la entrada correspondiente de la tabla 117 es suprimida y es preciso de nuevo revisar la memoria 110.

En otra variante, las autorizaciones de acceso y los derechos de acceso pueden ser asignados para un espacio geográfico predeterminado, el hecho de que el móvil salga de las condiciones definidas por el espacio geográfico conlleva automáticamente la liberación del recurso. La condición de uso ligada a este espacio geográfico puede ser definida de manera similar a la definición de las duraciones de uso, es decir de manera atómica o global por recurso y/o por aplicaciones, para varios recursos y/o varias aplicaciones.

En una variante de la invención la autorización de un número predeterminado N de accesos, puede ser dada de manera similar a la definición de las duraciones de uso, es decir de manera atómica o global por recurso y/o por aplicación, para varios recursos y/o para varias aplicaciones.

En la medida en la que la propia memoria 110 es un recurso, su acceso, particularmente en modificación, está sometido al mismo mecanismo de autorización. Se observa aquí que una memoria, por ejemplo la memoria 114, puede corresponder a varios recursos, agrupando un recurso los registros correspondientes a funcionalidades de operador de red, agrupando un recurso los registros correspondientes a funcionalidades de usuario, agrupando un recurso los registros correspondientes a funcionalidades de constructor del móvil y agrupando un recurso los registros correspondientes a funcionalidades de suministrador de contenidos. Cada uno de estos recursos es actualizado mediante una aplicación particular no pudiendo ser lanzado más que por, respectivamente, el operador de red, el usuario, el sistema de explotación y el suministrador de contenidos.

En una variante de la invención, el registro 114 comprende un campo 115 que identifica al propietario. En esta variante una aplicación que busca modificar el contenido del registro 114 no puede hacerlo si la citada aplicación y el registro 114 tienen el mismo propietario.

Estos mecanismos de seguridad permiten gestionar eficazmente la seguridad del teléfono permitiendo una compartimentación de los recursos por propietario de estos recursos, es decir que sólo el propietario de un recurso puede modificar los derechos de acceso a este recurso.

Estos mecanismos permiten una gran flexibilidad en la gestión de los derechos de uso, puesto que una aplicación identificada por el sistema de explotación y gestionada por el módulo 111 puede también ser identificada como un recurso del teléfono, esto es particularmente verdad en el marco de la telecarga de juegos. Siendo un juego a la vez una aplicación con los derechos restringidos y debiendo un recurso estar protegido contra la copia y el uso abusivo.

Así una aplicación que busca introducir, por medio de una interfaz de serie (por ejemplo Bluetooth), datos en el teléfono 101 deberá estar en la lista de las aplicaciones autorizadas para escribir en una cierta zona de memoria y en la lista de las aplicaciones autorizadas para leer la zona de memoria correspondiente a una memoria de tampón de recepción de los datos recibidos por medio de la interfaz de serie.

Una aplicación que busca hacer salir, por medio de una interfaz de serie por ejemplo, datos en el teléfono 101 deberá estar en la lista de las aplicaciones autorizadas a escribir en una cierta zona de memoria, correspondiente a una memoria tampón de emisión de los datos por medio de la interfaz de serie. En una variante, el módulo de interfaz de serie es un recurso y una aplicación que desea emitir datos deberá estar en la lista de las aplicaciones autorizadas a poner en práctica el módulo de interfaz de serie. En este ejemplo un usuario que desee emitir datos por medio de la interfaz de serie deberá utilizar una aplicación autorizada por una parte a leer estos datos, es decir que la aplicación tendrá derechos registrados en estos datos o recursos y por otra parte, emitir datos por medio de la interfaz de serie. Aquí la interfaz de serie es elegida a título de ejemplo, otra interfaz de comunicación puede ser utilizada como ilustración de la invención como el Wifi, el infrarrojo o las diversas posibilidades de extensión de memoria externa (incluso el bus externo del 2). Esto es particularmente interesante para la protección de las obras de multimedia. En efecto, es suficiente que la aplicación de reproducción ("player" en inglés) de la obra no sea autorizada a reproducir la obra de otra manera que por medio de un altavoz y/o una pantalla, para impedir que la obra sea extraída del teléfono. De la misma manera, si la obra está identificada como un recurso, sólo la aplicación de reproducción ("player" en inglés) podrá acceder a ella y modificarla, no estando ya los sistemas de gestión de ficheros autorizados a manipular las obras digitales, ninguna manipulación de ficheros de estas obras podrá ser realizada más que a través de la aplicación de reproducción. En una óptica de gestión de los derechos digitales, si se considera que una aplicación de reproducción está distribuida a gran escala y que esta aplicación está asociada a varios certificados electrónicos (un certificado por editor del disco o del cine), el hecho de definir una obra digital como un recurso asociado a certificados electrónicos conocidos de la aplicación o del teléfono implicará que sólo la aplicación puede acceder a estas obras. En este marco, siendo el propietario de la aplicación y de los recursos (obras codificadas digitalmente) el suministrador del contenido, ni el usuario del teléfono, ni el operador, ni el constructor, ni los otros suministradores de contenidos pueden alterar los derechos asociados a esta aplicación y a los recursos (obras codificadas digitalmente).

En una variante de la invención, una aplicación del constructor instalada en el móvil tiene el derecho de leer, escribir y borrar todas las zonas de memorias reservadas al uso del móvil (purgado o limpieza de una zona de memoria). En una variante de la invención puede situarse una validación del usuario de esta aplicación.

De manera que se optimice la utilización de la invención durante la instalación de una nueva aplicación en el teléfono móvil, esta aplicación es analizada de manera que se detecten todas las llamadas a recursos del teléfono. El identificador de la nueva aplicación es entonces inscrito en las tablas de identificadores en función bien sea de los derechos por defecto, bien sea de respuestas a preguntas planteadas al usuario del teléfono. La aplicación de análisis de las aplicaciones tiene por consiguiente los derechos requeridos para acceder al recurso correspondiente a la gestión de derechos. Esta aplicación forma parte del sistema de explotación.

En una variante de la invención el teléfono 101 comprende un programa, instalado por el constructor, pudiendo leer, escribir y borrar todas las zonas de memoria del móvil. Tal programa es, por ejemplo, un programa de reinicialización.

REIVINDICACIONES

1. Procedimiento para gestionar de manera segura la ejecución de aplicaciones en un teléfono (101) móvil, accediendo una aplicación (108c) a recursos (108a) del teléfono móvil gestionados mediante un sistema de explotación, **caracterizado** porque:

- diferentes recursos del teléfono móvil son identificables y están asociados cada uno a una tabla, comprendiendo la citada tabla identificadores de aplicaciones asociados a derechos de acceso al recurso, durante la instalación de la aplicación, la citada aplicación es analizada de manera que se detectan todas las llamadas a recursos del teléfono, y que inscribe en las tablas el identificador de la aplicación en función bien de los derechos por defecto, bien de respuestas a preguntas planteadas al usuario del teléfono,

- teniendo el recurso un propietario (115) autorizado sólo a modificar cada derecho de acceso a este recurso tras la citada instalación,

- buscando el sistema de explotación y aplicando para cada recurso al que se accede los derechos correspondientes a cada ocurrencia de aplicación que accede, comprendiendo cada aplicación un identificador (idAp) único.

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque el sistema de explotación gestiona una tabla dinámica y temporal por identificador de aplicación que permite mantener las autorizaciones de uso de los recursos ya autorizados para cada una de las aplicaciones.

3. Procedimiento de acuerdo con la reivindicación 2, **caracterizado** porque el sistema de explotación libera las autorizaciones de acceso a un recurso para la aplicación identificada al final del tiempo asignado, o a la salida de un espacio geográfico predeterminado.

4. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado** porque los recursos del sistema de explotación comprenden memorias y/o zonas de memorias del teléfono móvil.

5. Procedimiento de acuerdo con una de las reivindicaciones 1 a 4, **caracterizado** porque los recursos del sistema de explotación comprenden los medios de comunicaciones para el teléfono móvil.

6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado** porque el acceso a los recursos está centralizado al nivel de una interfaz de programa, permitiendo esta interfaz el acceso a un recurso si la aplicación que busca acceder a este recurso posee los derechos requeridos.

7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 6, **caracterizado** porque cada tabla de identificadores de aplicaciones asociada a un recurso comprende un identificador (116) correspondiente a las aplicaciones no listadas en la tabla para definir los derechos por defecto de una aplicación.

8. Procedimiento de acuerdo con una de las reivindicaciones 1 a 7, **caracterizado** porque los derechos por defecto pueden estar definidos para los accesos a los recursos de un mismo propietario, pudiendo esta definición ser realizada durante la configuración del móvil a la salida de fabricación.

9. Procedimiento de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado** porque una tabla de identificadores que comprende entradas correspondientes a certificados electrónicos permite agrupar bajo un mismo propietario a varias familias de certificados electrónicos.

10. Procedimiento de acuerdo con una de las reivindicaciones 1 a 9, **caracterizado** porque un acceso a un recurso está comprendido en el conjunto que comprende al menos los elementos siguientes: lectura, escritura, modificación, destrucción, ejecución, de datos o de código ejecutable.

11. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado** porque cuando se descuelga el teléfono un programa de descuelgue verifica la integridad de las tablas de identificadores y de la parte del sistema de explotación que accede a estas tablas de identificadores.

12. Procedimiento de acuerdo con una de las reivindicaciones 1 a 11, **caracterizado** porque cuando se descuelga el teléfono un programa de descuelgue verifica la integridad de las partes del sistema de explotación a cargo de las funciones de control y de seguridad del teléfono, permitiendo estos controles garantizar cuando se descuelga el móvil que sólo y exclusivamente el sistema de explotación original del constructor está instalado en el teléfono y es utilizado por éste.

13. Procedimiento de acuerdo con una de las reivindicaciones 1 a 12, **caracterizado** porque un derecho de acceso a un recurso está comprendido en el conjunto que comprende al menos los elementos siguientes: acceso autorizado, acceso autorizado una vez, acceso autorizado N veces, siendo N parametrizable, acceso denegado, solicitar la autorización al usuario una vez, solicitar la autorización al usuario para cada acceso, solicitar la autorización al usuario para

N accesos, siendo N parametrizable, solicitar la asignación de un código una vez, solicitar la asignación de un código para cada acceso, solicitar la asignación de un código para N accesos, siendo N parametrizable, solicitar un cálculo o un enigma criptográfico para autorizar el acceso una vez, solicitar un cálculo o un enigma criptográfico para autorizar cada acceso, solicitar un cálculo o un enigma criptográfico para autorizar N accesos, siendo N parametrizable.

14. Procedimiento de acuerdo con una de las reivindicaciones 1 a 13, **caracterizado** porque la tabla de identificadores de aplicaciones tiene un tamaño dinámico.

15. Procedimiento de acuerdo con una de las reivindicaciones 1 a 14, **caracterizado** porque cada nueva aplicación es analizada para actualizar las tablas de identificadores de aplicaciones.

16. Procedimiento de acuerdo con una de las reivindicaciones 1 a 15, **caracterizado** porque una aplicación del constructor instalada en el móvil tiene el derecho de leer, escribir, borrar todas las zonas de memorias reservadas para el uso del móvil.

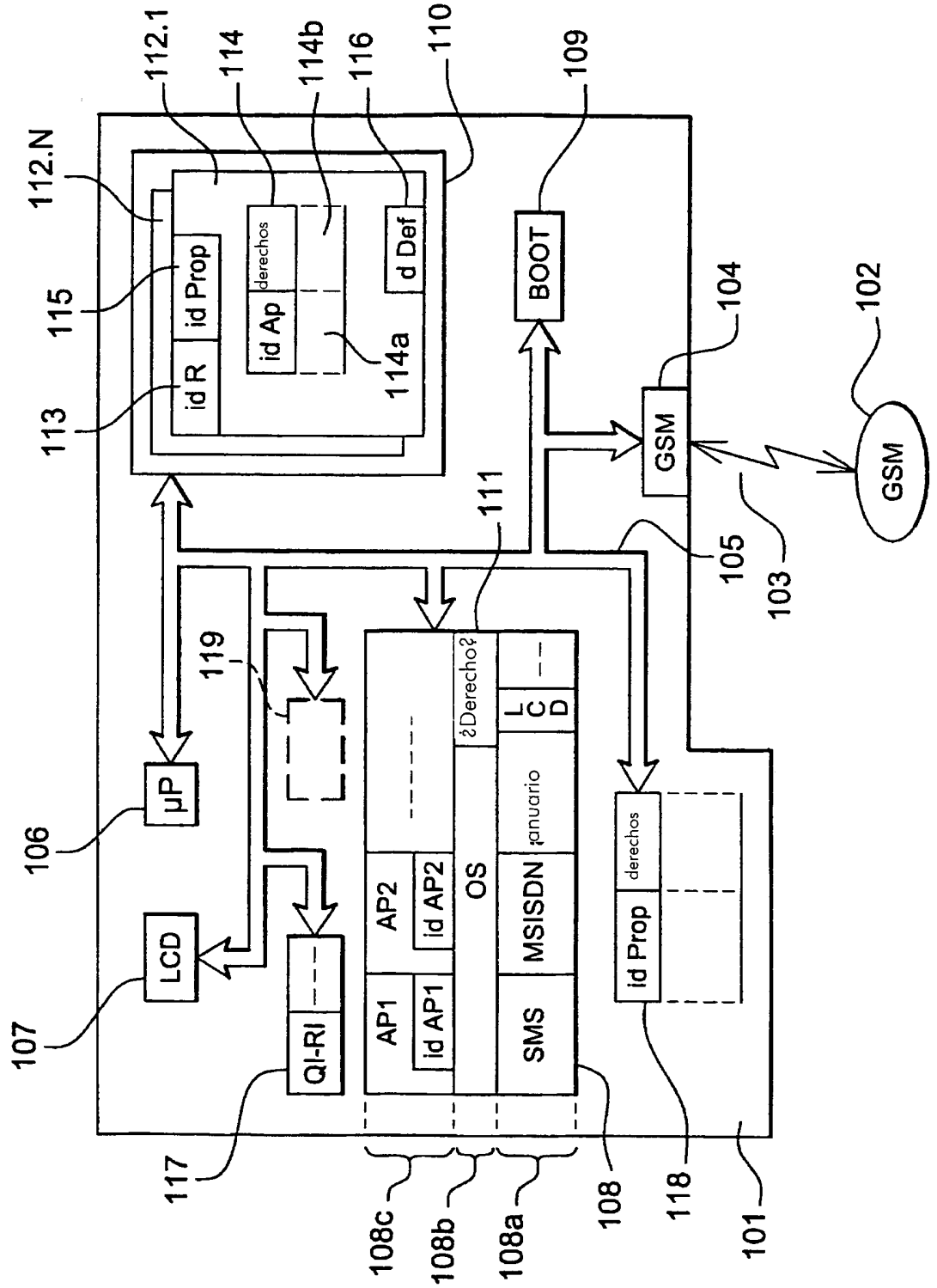
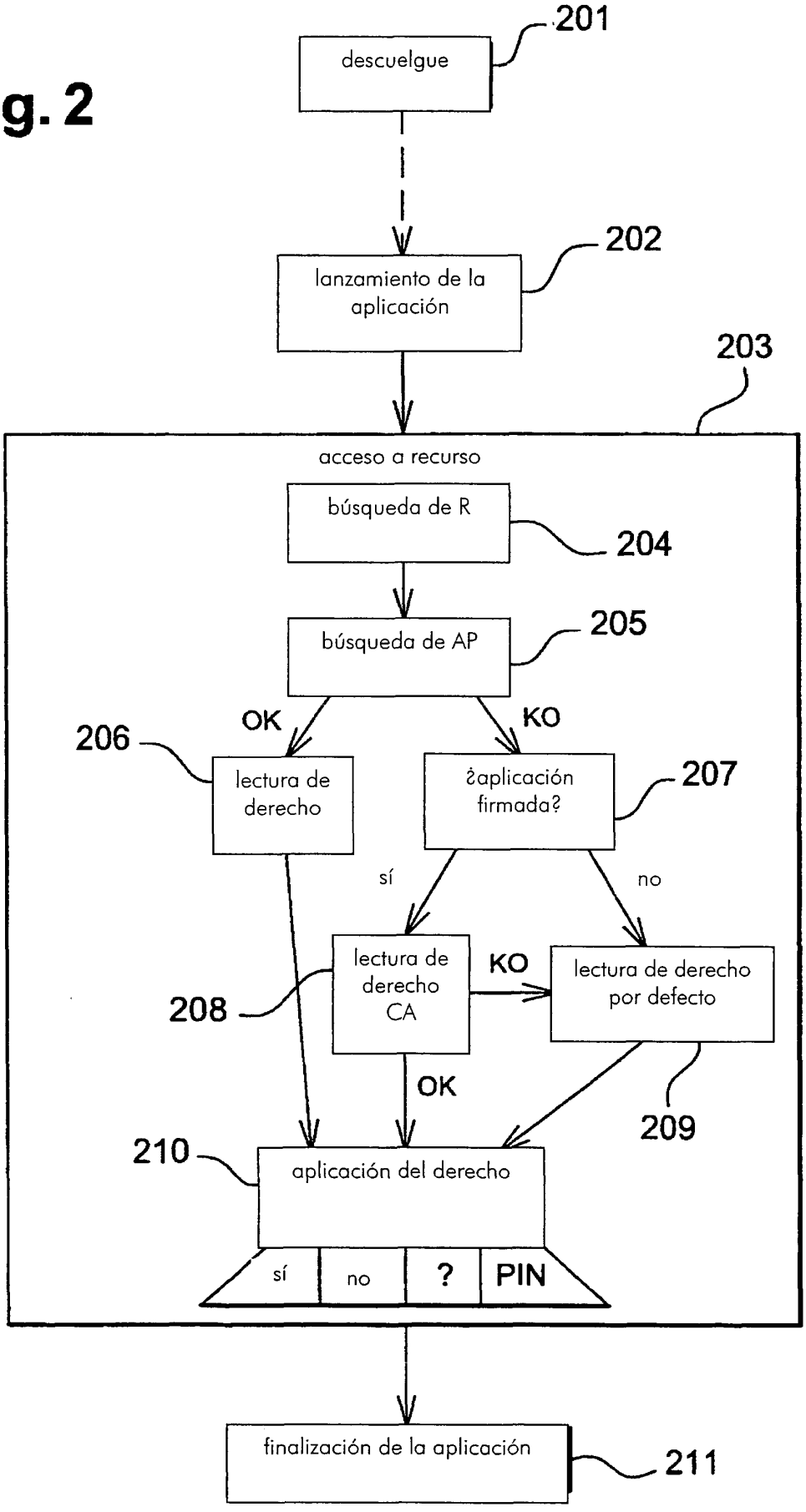

112.1
114
114b
116
110
109
112.N
115
113
id Prop
id R
id Ap
derechos
d Def
114a
BOOT
104
102
GSM
GSM
111
105
103
119
µP
106
LCD
107
QI-RI
117
AP1
id AP1
AP2
id AP2
OS
¿Derecho?
LCD
¿nuario
MSISDN
SMS
id Prop
derechos
108c
108b
108a
108
118
101

Fig. 1

Fig. 2


descuelgue
201
lanzamiento de la aplicación
202
203
acceso a recurso
búsqueda de R
204
búsqueda de AP
205
OK
KO
206
lectura de derecho
¿aplicación firmada?
207
sí
no
lectura de derecho CA
KO
lectura de derecho por defecto
208
OK
209
210
aplicación del derecho
sí
no
?
PIN
finalización de la aplicación
211