(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 770 006**

(51) Int. CI.:

***H04W 12/02*** (2009.01)
***H04W 12/06*** (2009.01)
***H04W 4/50*** (2008.01)
***H04W 4/60*** (2008.01)
***H04W 4/00*** (2008.01)
***H04W 12/12*** (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.09.2016 PCT/EP2016/070961**

(87) Fecha y número de publicación internacional: **20.04.2017 WO17063790**

(96) Fecha de presentación y número de la solicitud europea: **06.09.2016 E 16760730 (8)**

(97) Fecha y número de publicación de la concesión europea: **30.10.2019 EP 3363215**

(54) Título: **Método para gestionar una aplicación**

(30) Prioridad:

**16.10.2015 EP 15306660**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**30.06.2020**

(73) Titular/es:

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

(72) Inventor/es:

**FOKLE, MILAS;**
**GONZALVO, BENOIT y**
**HUYSMANS, GUILLAUME**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Método para gestionar una aplicación

**(Campo de la invención)**

La presente invención se refiere a métodos para gestionar aplicaciones. En particular, se refiere a métodos para gestionar aplicaciones destinadas a ser ejecutadas de forma segura en dispositivos.

**(Antecedentes de la invención)**

En el contexto de aplicación para dispositivos portátiles, cada vez se instalan más aplicaciones de *software*. Algunas de estas aplicaciones permiten acceder a datos o servicios sensibles, como el pago móvil por ejemplo. Existe el riesgo de que una persona malévola duplique una aplicación de *software* de un dispositivo a otro y utilice la aplicación para transacciones fraudulentas.

Existe la necesidad de aumentar la protección de las aplicaciones de *software* en los dispositivos.

El documento US 2014/0099925 A1 divulga un método para actualizar componentes del sistema operativo de un aparato inalámbrico.

**(Compendio de la invención)**

La invención está definida por las reivindicaciones 1, 6 y 10.

Un objeto de la invención es solucionar el problema técnico antes mencionado.

Un objeto de la presente invención es un método para gestionar una aplicación que incluye tanto una parte genérica como una parte adicional. La parte genérica está instalada en un dispositivo. El método comprende las siguientes etapas:

- el dispositivo obtiene una huella digital del dispositivo e inicia una autenticación de un usuario del dispositivo y, en caso de una autenticación satisfactoria, envía a un servidor una petición para obtener la parte adicional, comprendiendo la petición bien credenciales asociadas con el usuario, bien una referencia del usuario, la huella digital y una referencia de la aplicación,

- el servidor identifica la parte adicional, genera una parte cifrada de la parte adicional utilizando una clave basada tanto en las credenciales como en la huella digital y construye un programa de autodescifrado configurado para descifrar la parte cifrada,

- el dispositivo recibe la parte cifrada y el programa de autodescifrado,

- el dispositivo obtiene la huella digital y las credenciales y recupera la parte adicional ejecutando el programa de autodescifrado con dichas huella digital y credenciales como parámetros de entrada.

Ventajosamente, el dispositivo puede almacenar la parte cifrada y el programa de autodescifrado en su memoria no volátil, el dispositivo puede obtener la huella digital e iniciar una autenticación del usuario y, en caso de una autenticación satisfactoria, el dispositivo puede obtener las credenciales y ejecutar el programa de autodescifrado en cuanto vaya a ejecutarse la parte adicional.

Ventajosamente, el dispositivo puede obtener la huella digital del dispositivo y una referencia de usuario y puede enviar a un servidor de control una petición de uso que comprenda las credenciales o una referencia del usuario, la huella digital y la referencia de la aplicación. El servidor de control puede comprobar si el usuario tiene permiso para ejecutar la aplicación y envía un resultado que refleja la comprobación al dispositivo. El dispositivo puede autorizar o no la ejecución de la aplicación dependiendo del resultado recibido.

Ventajosamente, el dispositivo puede tener un entorno de tiempo de ejecución variable. La petición puede comprender una característica que refleje el estado del entorno de tiempo de ejecución actual y la petición puede enviarse en cuanto vaya a ejecutarse la parte adicional.

Ventajosamente, el servidor puede seleccionar dinámicamente un algoritmo de cifrado entre una pluralidad de algoritmos de cifrado para generar la parte cifrada.

Otro objeto de la presente invención es un dispositivo capaz de comunicarse con un servidor. El dispositivo está configurado para recibir e instalar una parte genérica de una aplicación. El dispositivo comprende un agente configurado para obtener una huella digital del dispositivo y para iniciar una autenticación de un usuario del dispositivo y, en caso de una autenticación satisfactoria, recuperar credenciales asociadas con el usuario. El agente está configurado para enviar al servidor una petición para obtener una parte adicional de la aplicación. La petición comprende las credenciales o una referencia del usuario, la huella digital y una referencia de la aplicación. El agente está configurado para recibir del servidor un programa de autodescifrado asociado a la aplicación y para recuperar la

parte adicional ejecutando el programa de autodescifrado con la huella digital y las credenciales como parámetros de entrada.

Ventajosamente, el dispositivo puede estar configurado para almacenar la parte cifrada y el programa de autodescifrado en su memoria no volátil. El agente puede estar configurado para iniciar una autenticación del usuario y, en caso de una autenticación satisfactoria, obtener la huella digital y las credenciales y ejecutar el programa de autodescifrado en cuanto vaya a ejecutarse la parte adicional.

Ventajosamente, el agente puede estar configurado para enviar a un servidor de control una petición de uso que comprenda las credenciales o una referencia del usuario, la huella digital y la referencia de la aplicación. El agente puede estar configurado para autorizar o no la ejecución de la aplicación dependiendo de un resultado recibido del servidor de control en respuesta a la petición de uso.

Ventajosamente, el dispositivo tiene un entorno de tiempo de ejecución variable y el agente puede estar configurado para añadir a la petición una característica que refleje el estado actual del entorno de tiempo de ejecución variable. El agente puede estar configurado para enviar la petición en cuanto vaya a ejecutarse la parte adicional.

Otro objeto de la presente invención es un servidor capaz de participar en el despliegue de una aplicación que incluye dos partes: una parte genérica y una parte adicional. La parte genérica está previamente instalada en un dispositivo. El servidor comprende un agente de comprobación adaptado para recibir una petición para obtener la parte adicional. La petición comprende credenciales asociadas con un usuario del dispositivo o una referencia de un usuario del dispositivo, una huella digital del dispositivo y una referencia de la aplicación. El servidor comprende un agente de descubrimiento adaptado para identificar la parte adicional. El servidor comprende un agente de generación adaptado para generar una parte cifrada de la parte adicional utilizando una clave basada tanto en las credenciales como en la huella digital. El servidor comprende un agente de cifrado adaptado para construir un programa de autodescifrado configurado para descifrar la parte cifrada y para enviar tanto la parte cifrada como el programa de autodescifrado en respuesta a la petición.

**(Breve descripción de los dibujos)**

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

- la Figura 1 es un diagrama de flujo que muestra un ejemplo de instalación de una aplicación en un dispositivo según la invención,

- la Figura 2 es un diagrama de flujo que muestra un ejemplo de control de ejecución de una aplicación en un dispositivo según la invención,

- la Figura 3 muestra un ejemplo de diseño de aplicación gestionada según la invención,

- la Figura 4 muestra un ejemplo de arquitectura de un dispositivo configurado para gestionar aplicaciones según la invención, y

- la Figura 5 muestra un ejemplo de arquitectura de un servidor configurado para gestionar aplicaciones según la invención.

**(Descripción detallada de las realizaciones preferidas)**

La invención puede aplicarse a cualesquiera tipos de dispositivos capaces de comunicarse con un servidor remoto y destinados a ejecutar una aplicación de *software*. En particular, la invención es adecuada para aplicaciones de *software* que se ejecuten en dispositivos portátiles tales como teléfonos móviles, PC tipo tableta, gafas electrónicas, relojes electrónicos y pulseras electrónicas. También puede aplicarse a cualquier dispositivo como un vehículo, un contador, una máquina tragaperras, un televisor o un ordenador.

La Figura 1 muestra un ejemplo de método para gestionar una aplicación de *software* según la invención.

En este ejemplo, el dispositivo DE1 es un teléfono móvil que tiene su propio sistema operativo, como Android® por ejemplo.

La aplicación A1 de *software* está diseñada de manera que comprende dos partes complementarias: una parte genérica BT y una parte adicional P1.

Preferiblemente, la parte genérica BT puede ser una parte de *software* que pueda utilizarse para varias clases de aplicación. Puede comprender características y componentes comunes a varias aplicaciones.

La parte genérica BT está separada del sistema operativo del dispositivo DE1.

Ventajosamente, la parte genérica BT puede estar desarrollada como una secuencia inicial de instrucciones capaz de gestionar la descarga de la parte adicional P1.

En una primera etapa, un servidor SV2 envía la parte genérica BT al dispositivo DE1 y se instala la parte genérica BT en el dispositivo DE1. En una realización, la parte genérica BT puede recuperarse e instalarse libremente desde el servidor SV2.

En una segunda etapa, el dispositivo DE1 autentica el usuario. Por ejemplo, el dispositivo DE1 puede pedir al usuario que introduzca un código PIN o una contraseña específica a través de la pantalla/el teclado del dispositivo DE1. El dispositivo DE1 puede también obtener una medición biométrica del usuario. Como alternativa, el usuario puede autenticarse utilizando datos secretos recuperados de otro dispositivo en el que estén almacenados esos datos secretos. Este otro dispositivo puede ser un testigo USB o un testigo NFC (*Near Field Communication* (comunicación de campo próximo)), por ejemplo. En caso de una autenticación satisfactoria del usuario, el dispositivo DE1 obtiene credenciales UC del usuario.

En una tercera etapa, el dispositivo DE1 recupera una huella digital DFP del dispositivo DE1 y construye una petición R1 que comprende las credenciales UC del usuario, la huella digital DFP y una referencia AppID a la aplicación A1.

En otro ejemplo, las credenciales UC pueden derivarse de una credencial maestra, de manera que las credenciales UC utilizadas se diversifiquen para cada transacción. En este caso, el dispositivo DE1 recupera la credencial maestra de su propia memoria y genera un testigo derivado que se utiliza como credenciales UC.

En otro ejemplo, el dispositivo DE1 puede construir una petición R1 que comprenda una referencia (es decir un identificador) del usuario en lugar de las credenciales UC del usuario. En este caso, se supone que las credenciales UC están previamente almacenadas en ambos lados: el servidor y el dispositivo DE1.

En otro ejemplo, las credenciales UC pueden derivarse de los datos secretos utilizados (por ejemplo proporcionados) por el usuario para autenticarse ante el dispositivo DE1.

La referencia AppID puede ser un identificador o el nombre de la aplicación A1, por ejemplo. La huella digital DFP puede ser un número de serie del dispositivo DE1 o cualquier dato específico del dispositivo DE1.

Ventajosamente, la huella digital DFP puede generarse sobre la base de varias mediciones o elementos del dispositivo DE1. Por ejemplo, la huella digital DFP puede construirse a partir de una combinación del número (y/o nombre) de aplicaciones instaladas en el dispositivo DE1 y el tamaño de la memoria no volátil (NVM, por sus siglas en inglés) libre remanente del dispositivo DE1.

A continuación, el dispositivo DE1 envía la petición R1 a un servidor SV1 para obtener la parte adicional P1.

En una cuarta etapa, el servidor SV1 identifica la parte adicional P1 sobre la base de la referencia AppID. El servidor SV1 puede o generar o recuperar de un almacenamiento dedicado la parte adicional P1. A continuación, el servidor SV1 genera una parte cifrada EP1 de la parte adicional P1 utilizando como parámetros de entrada tanto las credenciales UC del usuario como la huella digital DFP. El servidor SV1 construye también un programa AP1 de autodescifrado diseñado para descifrar la parte cifrada EP1.

Como alternativa, el servidor SV1 puede calcular una clave basándose tanto en las credenciales UC del usuario como en la huella digital DFP y puede generar la parte cifrada EP1 utilizando esta clave calculada.

En una realización, el servidor SV1 puede utilizar un algoritmo de cifrado preestablecido para generar la parte cifrada EP1. Opcionalmente, el servidor SV1 puede seleccionar dinámicamente un algoritmo de cifrado entre varios algoritmos de cifrado para generar la parte cifrada EP1, de manera que el algoritmo de cifrado utilizado puede ser distinto de una vez a otra. Por ejemplo, el servidor SV1 puede seleccionar aleatoriamente bien un algoritmo AES (*Advanced Encryption Standard* (estándar de cifrado avanzado)), bien un algoritmo XOR.

El programa AP1 de autodescifrado es una aplicación de *software* autónoma que está configurada para descifrar la parte cifrada EP1. Necesita como parámetros de entrada tanto las credenciales UC del usuario como la huella digital DFP.

En una quinta etapa, el servidor SV1 envía tanto la parte cifrada EP1 como el programa AP1 de autodescifrado en respuesta a la petición R1. Preferiblemente, el dispositivo DE1 puede obtener estos dos elementos en un único paquete. Opcionalmente, estos dos elementos pueden ser recibidos en dos paquetes.

Desde este punto, hay dos opciones posibles. Bien el paquete (que comprende tanto la parte cifrada EP1 como el programa AP1 de autodescifrado) se almacena en la memoria no volátil del dispositivo DE1 y se utilizará más tarde, bien se utiliza inmediatamente para ejecutar la aplicación A1 sin ser almacenado de forma permanente en el dispositivo DE1.

En la primera opción, cada vez que la parte adicional P1 vaya a arrancar (es decir en cuanto vaya a ejecutarse la parte adicional P1), el dispositivo DE1 autentica el usuario y, en caso de una autenticación satisfactoria, obtiene de nuevo

las credenciales UC del usuario y la huella digital DFP del dispositivo DE1. Luego, el dispositivo DE1 lanza la ejecución del programa AP1 de autodescifrado utilizando las credenciales UC del usuario y la huella digital DFP como parámetros de entrada para recuperar la parte adicional P1. El dispositivo DE1 almacena la parte adicional P1 en su memoria de trabajo, que se borra cuando se reinicia o se apaga el dispositivo DE1.

Gracias a esta opción, aunque el paquete (que comprende tanto la parte cifrada EP1 como el programa AP1 de autodescifrado) se copie ilegalmente del dispositivo DE1 a otro dispositivo, la parte adicional P1 no puede recuperarse en este otro dispositivo porque la huella digital será diferente y las credenciales del usuario no estarán disponibles.

En la segunda opción, el dispositivo DE1 recupera inmediatamente (es decir en cuanto se haya recibido el programa AP1 de autodescifrado) la parte adicional P1 ejecutando el programa AP1 de autodescifrado utilizando las credenciales UC del usuario y la huella digital DFP como parámetros de entrada sin una segunda autenticación del usuario. En la segunda opción, el dispositivo no almacena de manera permanente el programa AP1 de autodescifrado, la parte cifrada EP1 ni la parte adicional P1 en su memoria no volátil.

Opcionalmente, el dispositivo DE1 puede recuperar una característica RTP específica del estado actual de su entorno de tiempo de ejecución e insertar esta característica RTP en la petición R1. El servidor SV1 puede estar diseñado para generar una parte adicional P1 que pueda utilizarse sólo con el entorno de tiempo de ejecución actual del dispositivo DE1. En otras palabras, la parte adicional P1 se personaliza para que pueda ser utilizada sólo por el entorno de tiempo de ejecución actual del dispositivo DE1. Por ejemplo, la característica RTP puede ser la primera dirección del área de memoria asignada para ejecutar la parte adicional P1. El entorno de tiempo de ejecución del dispositivo DE1 se considera suficientemente variable para que la parte adicional P1 personalizada no pueda utilizarse posteriormente (es decir cuando haya cambiado el estado del entorno de tiempo de ejecución) en el dispositivo DE1 ni en otro dispositivo.

En este caso, la parte adicional P1 se personaliza de acuerdo con el estado del entorno de tiempo de ejecución de destino.

Para reforzar el nivel de seguridad, el servidor SV1 y el dispositivo DE1 pueden establecer un canal seguro antes de intercambiar la petición R1 y su respuesta. Por ejemplo, pueden comunicarse a través de un canal OTA (*Over-The-Air* (por el aire)) 3G o 4G o a través de una sesión HTTPS.

Aunque en los ejemplos descritos anteriormente los servidores SV1 y SV2 se muestran como dos entidades separadas, pueden estar unidos en un solo servidor o máquina.

La Figura 2 muestra un ejemplo de método para controlar la ejecución de una aplicación de *software* según la invención.

En este ejemplo, el dispositivo DE1 puede ser un PC tipo tableta y la aplicación A1 puede ser similar a la aplicación descrita en la Figura 1.

Este método se refiere a la primera opción anteriormente descrita (es decir cuando la parte cifrada EP1 y el programa AP1 de autodescifrado están almacenados de manera permanente en la memoria no volátil del dispositivo DE1).

En cuanto la parte adicional P1 esté a punto de ser ejecutada, el dispositivo DE1 autentica el usuario y, en caso de una autenticación satisfactoria, obtiene las credenciales UC del usuario. Por ejemplo, puede recuperar las credenciales UC desde un segundo dispositivo DE2 que almacene estas credenciales. Por ejemplo, el dispositivo DE2 puede ser un dispositivo capaz de comunicarse con el dispositivo DE1 a través de una sesión inalámbrica, como NFC, Wifi o Bluetooth®.

El dispositivo DE1 recupera una huella digital DFP del dispositivo DE1 y construye una petición R2 de uso, que comprende las credenciales UC del usuario (o una referencia del usuario), la huella digital DFP y una referencia AppID a la aplicación A1. Luego, el dispositivo DE1 envía la petición R2 de uso a un servidor SV3 para obtener autorización para ejecutar la parte adicional P1.

El servidor SV3 identifica la parte adicional P1 (y por lo tanto la aplicación A1) basándose en la AppID de referencia. Luego, el servidor SV3 comprueba si el usuario cuyas credenciales UC (o una referencia) se han recibido está autorizado para ejecutar la parte adicional P1 (es decir para ejecutar la aplicación A1) en el dispositivo correspondiente a la huella digital DFP. Esta comprobación puede estar basada en una cuenta asignada al usuario. Puede estar basada en un número limitado de ejecución o ejecuciones y/o un intervalo de tiempo.

Luego, el servidor SV3 envía al dispositivo DE1 una respuesta que refleja el resultado de la comprobación. En caso de una comprobación satisfactoria el dispositivo DE1 autoriza la ejecución de la parte adicional P1, de lo contrario deniega la ejecución de la parte adicional P1.

En un ejemplo, el programa AP1 de autodescifrado puede estar configurado para denegar el descifrado de la aplicación adicional P1 si el resultado proporcionado por el servidor SV3 es negativo.

En otro ejemplo, la parte genérica BT puede estar configurada para denegar la ejecución de la parte adicional P1 en caso de que el servidor SV3 envíe un mal resultado.

En un tercer ejemplo, el servidor SV3 puede enviar datos cuyo valor sea utilizado como parámetro de entrada por el programa AP1 de autodescifrado.

Opcionalmente, el servidor SV3 y el servidor SV1 de la Figura 1 pueden estar unidos en un solo servidor o máquina.

La Figura 3 muestra un ejemplo de arquitectura de la aplicación A1 gestionada según la invención.

La aplicación A1 de *software* comprende dos partes requeridas para la ejecución correcta de la aplicación: una parte genérica BT y una parte adicional P1.

La parte genérica BT está diseñada específicamente para la aplicación A1. La parte genérica BT es específica de la aplicación A1.

La parte genérica BT puede considerarse como una aplicación incompleta que necesita la parte adicional P1 para convertirse enteramente en la aplicación A1 completa.

Hay que señalar que la parte genérica BT no es ni un elemento del sistema operativo ni una máquina virtual universal como Java RE. No es una librería compartible (como un DLL). Es un *software* autónomo que puede arrancarse independientemente y que requiere una parte adicional para ejecutar tratamientos deseados.

A la inversa, la parte adicional P1 no es un *software* autónomo que pueda arrancarse independientemente.

En un ejemplo, la parte genérica BT comprende características y datos aplicativos cuyo nivel de seguridad es bajo y la parte adicional P1 comprende características y datos aplicativos cuyo nivel de seguridad es alto.

En un ejemplo, la parte genérica BT comprende un gestor DM de descarga. El gestor DM de descarga está adaptado para gestionar la descarga de la parte adicional P1 desde un servidor remoto.

Gracias a la invención, la parte genérica BT puede registrarse como una aplicación única en una tienda de aplicaciones. Una flota de dispositivos puede obtener la parte genérica BT desde la tienda de aplicaciones y luego cargar de forma segura la parte adicional P1 personalizada para cada dispositivo.

La invención es aplicable a cualquier tipo de aplicación de *software*. Por ejemplo, la aplicación A1 puede estar dedicada a un control de acceso físico, identidad, pago, telecomunicaciones, fidelidad, o acceso a servicios como vídeos, fotos o música.

La Figura 4 muestra un ejemplo de arquitectura del dispositivo DE1 configurado para gestionar aplicaciones según la invención.

El dispositivo DE1 es similar al teléfono móvil de la Figura 1. El dispositivo DE1 incluye una memoria no volátil ME, que puede ser una memoria rápida (*flash*). El sistema operativo OS del dispositivo DE1, un agente AG y la parte genérica BT de la aplicación A1 están almacenados en la memoria no volátil ME. El dispositivo DE1 incluye también un entorno de tiempo de ejecución RTE, que puede comprender la parte adicional P1 (dibujada con línea de puntos) cuando ésta ha sido descifrada y está lista para el uso. El entorno de tiempo de ejecución RTE comprende una memoria de trabajo (por ejemplo RAM volátil).

El agente AG está configurado para recuperar una huella digital DFP del dispositivo DE1. Por ejemplo, el agente puede estar adaptado para leer un identificador (es decir el número de serie) del dispositivo DE1 o un identificador de un componente de *hardware* integrado únicamente en el dispositivo DE1 (como un disco duro o una pantalla, por ejemplo). El agente AG también está configurado para recuperar las credenciales UC asociadas a un usuario del dispositivo DE1. El agente AG también puede estar configurado para recuperar una referencia del usuario, como un identificador, un nombre o un número de abono. El agente AG está configurado para construir una petición R1 que comprenda las credenciales UC (o una referencia del usuario), la huella digital DFP y una referencia AppID de la aplicación A1. La referencia AppID puede ser un identificador de la aplicación A1, por ejemplo.

El agente AG también puede estar configurado para obtener unas credenciales maestras y para derivar las credenciales UC de las credenciales maestras (como testigo temporal o testigo de un solo uso, por ejemplo).

La petición R1 es una petición dirigida a obtener la parte adicional P1 de la aplicación A1 desde el servidor SV1. El agente AG está configurado también para recibir desde el servidor SV1 un programa AP1 de autodescifrado asociado a la aplicación A1 y para recuperar la parte adicional P1 ejecutando el programa AP1 de autodescifrado con la huella digital DFP y las credenciales UC como parámetros de entrada.

Ventajosamente, el agente AG puede estar configurado para obtener la huella digital DFP y las credenciales UC y para ejecutar el programa AP1 de autodescifrado en cuanto vaya a ejecutarse la parte adicional P1.

Ventajosamente, el agente AG puede estar configurado para comprobar la integridad del programa AP1 de autodescifrado recibido (y/o la parte cifrada EP1 recibida) y para obtener la huella digital DFP y las credenciales UC del usuario sólo en caso de una comprobación de integridad satisfactoria.

Ventajosamente, el agente AG puede estar configurado para enviar a un servidor SV3 de control una petición R2 de uso que comprenda las credenciales UC (o una referencia del usuario), la huella digital DFP y la referencia AppID de la aplicación A1. En este caso, el agente AG puede estar configurado también para autorizar o no la ejecución de la parte adicional P1 dependiendo del resultado recibido del servidor SV3 de control en respuesta a la petición R2 de uso.

Opcionalmente, el agente AG puede estar configurado para añadir a la petición R1 una característica RTP que refleje el estado actual del entorno de tiempo de ejecución RTE (es decir que sea específica del estado actual del RTE). El agente AG puede estar configurado también para enviar la petición R1 en cuanto vaya a ejecutarse la parte adicional P1.

En una realización, el agente AG y la parte genérica BT pueden estar unidos en una sola entidad. Por ejemplo, la parte genérica BT puede estar configurada para proporcionar todas las características del agente AG.

La Figura 5 muestra un ejemplo de arquitectura del servidor SV1 configurado para gestionar aplicaciones según la invención.

El servidor SV1 comprende un agente M1 de comprobación, un agente M2 de descubrimiento, un agente M3 de generación y un agente M4 de cifrado. El agente M1 de comprobación está configurado para recibir la petición R1 como se ha descrito en la Figura 1. El agente M2 de descubrimiento está configurado para identificar la parte adicional P1 basándose en la referencia AppID hallada en la petición R1. El agente M3 de generación está configurado para generar una parte cifrada EP1 de la parte adicional P1 utilizando tanto las credenciales UC del usuario (o la referencia del usuario) como la huella digital DFP del dispositivo hallada en la petición R1.

El agente M4 de cifrado está diseñado para construir un programa AP1 de autodescifrado configurado para descifrar la parte cifrada EP1 y para enviar tanto la parte cifrada EP1 como el programa AP1 de autodescifrado en respuesta a la petición R1.

El agente M3 de generación y el agente M4 de cifrado pueden utilizar un algoritmo de cifrado preestablecido o seleccionar un algoritmo de cifrado entre varios algoritmos de cifrado disponibles.

Estos cuatro agentes pueden implementarse como diferentes componentes de *software* o combinarse en uno o varios componentes.

Según la invención, una vez instalada en el dispositivo DE1 la parte adicional P1, ésta puede utilizarse siempre que no se apague o se reinicie el dispositivo, aunque se pierda la conexión con el servidor SV1. En otras palabras, el dispositivo DE1 podría quedarse fuera de línea mientras se ejecuta la aplicación A1.

Gracias a la invención, la ejecución de la parte adicional P1 (y por lo tanto de la aplicación A1) está protegida contra intentos fraudulentos, dado que siempre se realiza una autenticación del usuario y antes de iniciar la ejecución se requieren tanto credenciales del usuario como una huella digital del dispositivo. La invención proporciona una solución anticlonación.

La invención permite proporcionar un paquete diversificado (es decir parte cifrada EP1 y programa AP1 de autodescifrado) a todo usuario legítimo, mientras se proporciona la misma aplicación (es decir servicio) a todo usuario autorizado.

Debe entenderse, dentro del alcance de la invención, que las realizaciones anteriormente descritas se proporcionan como ejemplos no limitativos. En particular, el dispositivo puede ejecutar varias aplicaciones protegidas con la invención, y las aplicaciones de *software* pueden estar escritas en cualesquiera lenguajes.

La arquitectura del dispositivo DE1 y la arquitectura del servidor SV1 se proporcionan sólo a modo de ejemplo.

**REIVINDICACIONES**

1. Un método para gestionar una aplicación (A1), en donde dicha aplicación (A1) incluye dos partes: una parte genérica (BT) y una parte adicional (P1), instalándose dicha parte genérica (BT) en un dispositivo (DE1), comprendiendo dicho método las etapas:

- el dispositivo (DE1) obtiene una huella digital (DFP) del dispositivo (DE1) e inicia una autenticación de un usuario del dispositivo (DE1) y, en caso de una autenticación satisfactoria, envía a un servidor (SV1) una petición (R1) para obtener la parte adicional (P1), comprendiendo dicha petición (R1) bien credenciales (UC) asociadas con el usuario, bien una referencia del usuario, la huella digital (DFP) y una referencia (AppID) de la aplicación (A1),

- el servidor (SV1) identifica la parte adicional (P1), genera una parte cifrada (EP1) de la parte adicional (P1) utilizando una clave basada tanto en las credenciales (UC) como en la huella digital (DFP) y construye un programa (AP1) de autodescifrado configurado para descifrar la parte cifrada (EP1),

- el dispositivo (DE1) recibe la parte cifrada (EP1) y el programa (AP1) de autodescifrado desde el servidor (SV1),

- el dispositivo (DE1) obtiene la huella digital (DFP) y las credenciales (UC) y recupera la parte adicional (P1) ejecutando el programa (AP1) de autodescifrado con dichas huella digital (DFP) y credenciales (UC) como parámetros de entrada.

2. Un método según la reivindicación 1, en donde el dispositivo (DE1) almacena la parte cifrada (EP1) y el programa (AP1) de autodescifrado en su memoria no volátil, en donde el dispositivo (DE1) obtiene la huella digital (DFP) e inicia una autenticación del usuario y en donde, en caso de una autenticación satisfactoria, el dispositivo (DE1) obtiene las credenciales (UC) y ejecuta el programa (AP1) de autodescifrado en cuanto vaya a ejecutarse la parte adicional (P1).

3. Un método según la reivindicación 1, en donde el dispositivo (DE1) obtiene la huella digital (DFP) del dispositivo (DE1) y una referencia del usuario y envía a un servidor (SV3) de control una petición (R2) de uso que comprende las credenciales (UC) o una referencia del usuario, la huella digital (DFP) y la referencia (AppID) de la aplicación (A1),

- el servidor (SV3) de control comprueba si el usuario está autorizado para ejecutar la aplicación (A1) y envía un resultado que refleja la comprobación al dispositivo (DE1),

- el dispositivo (DE1) autoriza o no la ejecución de la aplicación (A1) dependiendo del resultado recibido.

4. Un método según la reivindicación 1, en donde el dispositivo (DE1) tiene un entorno de tiempo de ejecución variable, en donde dicha petición (R1) comprende una característica (RTP) que refleja el estado del entorno de tiempo de ejecución actual y en donde la petición (R1) se envía en cuando vaya a ejecutarse la parte adicional (P1).

5. Un método según la reivindicación 1, en donde el servidor (SV1) selecciona dinámicamente un algoritmo de cifrado entre una pluralidad de algoritmos de cifrado para generar la parte cifrada (EP1).

6. Un dispositivo (DE1) capaz de comunicarse con un servidor (SV1), estando el dispositivo (DE1) configurado para recibir e instalar una parte genérica (BT) de una aplicación (A1), comprendiendo dicho dispositivo (DE1):

- un agente (AG) configurado para obtener una huella digital (DFP) del dispositivo (DE1) y para iniciar una autenticación de un usuario del dispositivo (DE1), y, en caso de una autenticación satisfactoria, recuperar credenciales (UC) asociadas con el usuario, y para enviar a dicho servidor (SV1) una petición (R1) para obtener una parte adicional (P1) de la aplicación (A1), comprendiendo dicha petición (R1) las credenciales (UC) o una referencia del usuario, la huella digital (DFP) y una referencia (AppID) de la aplicación (A1), estando dicho agente (AG) configurado para recibir desde el servidor (SV1) una parte cifrada (EP1) y un programa (AP1) de autodescifrado asociado a la aplicación (A1), estando dicho programa (AP1) de autodescifrado configurado para descifrar la parte cifrada (EP1) y estando dicho agente (AG) configurado para recuperar la parte adicional (P1) ejecutando el programa (AP1) de autodescifrado con la huella digital (DFP) y las credenciales (UC) como parámetros de entrada.

7. Un dispositivo (DE1) según la reivindicación 6, estando el dispositivo (DE1) configurado para almacenar la parte cifrada (EP1) y el programa (AP1) de autodescifrado en su memoria no volátil y estando el agente (AG) configurado para iniciar una autenticación del usuario y, en caso de una autenticación satisfactoria, obtener la huella digital (DFP) y las credenciales (UC) y ejecutar el programa (AP1) de autodescifrado en cuanto vaya a ejecutarse la parte adicional (P1).

8. Un dispositivo (DE1) según la reivindicación 6, en donde el agente (AG) está configurado para enviar a un servidor (SV3) de control una petición (R2) de uso que comprende las credenciales (UC) o una referencia del usuario, la huella digital (DFP) y la referencia (AppID) de la aplicación (A1) y en donde el agente (AG) está configurado para autorizar o no la ejecución de la aplicación (A1) dependiendo de un resultado recibido del servidor (SV3) de control en respuesta a la petición (R2) de uso.

9. Un dispositivo (DE1) según la reivindicación 6, teniendo el dispositivo (DE1) un entorno de tiempo de ejecución variable, estando dicho agente (AG) configurado para añadir a la petición (R1) una característica (RTP) que refleja el

estado actual del entorno de tiempo de ejecución variable y estando el agente (AG) configurado para enviar la petición (R1) en cuanto vaya a ejecutarse la parte adicional (P1).

10. Un servidor (SV1) capaz de participar en el despliegue de una aplicación (A1), siendo dicho servidor (SV1) un aparato electrónico, incluyendo dicha aplicación (A1) dos partes: una parte genérica (BT) y una parte adicional (P1), suponiéndose que dicha parte genérica (BT) está previamente instalada en un dispositivo (DE1), comprendiendo el servidor (SV1) un agente (M1) de comprobación adaptado para recibir una petición (R1) para obtener la parte adicional (P1), comprendiendo dicha petición (R1) credenciales (UC) asociadas con un usuario del dispositivo (DE1) o una referencia de un usuario del dispositivo (DE1), una huella digital (DFP) del dispositivo (DE1) y una referencia (AppID) de la aplicación (A1),

comprendiendo el servidor (SV1) un agente (M2) de descubrimiento adaptado para identificar la parte adicional (P1), un agente (M3) de generación adaptado para generar una parte cifrada (EP1) de la parte adicional (P1) utilizando una clave basada tanto en las credenciales (UC) como en la huella digital (DFP), y un agente (M4) de cifrado adaptado para construir un programa (AP1) de autodescifrado configurado para descifrar la parte cifrada (EP1) y para enviar al dispositivo (DE1) tanto la parte cifrada (EP1) como el programa (AP1) de autodescifrado en respuesta a la petición (R1).

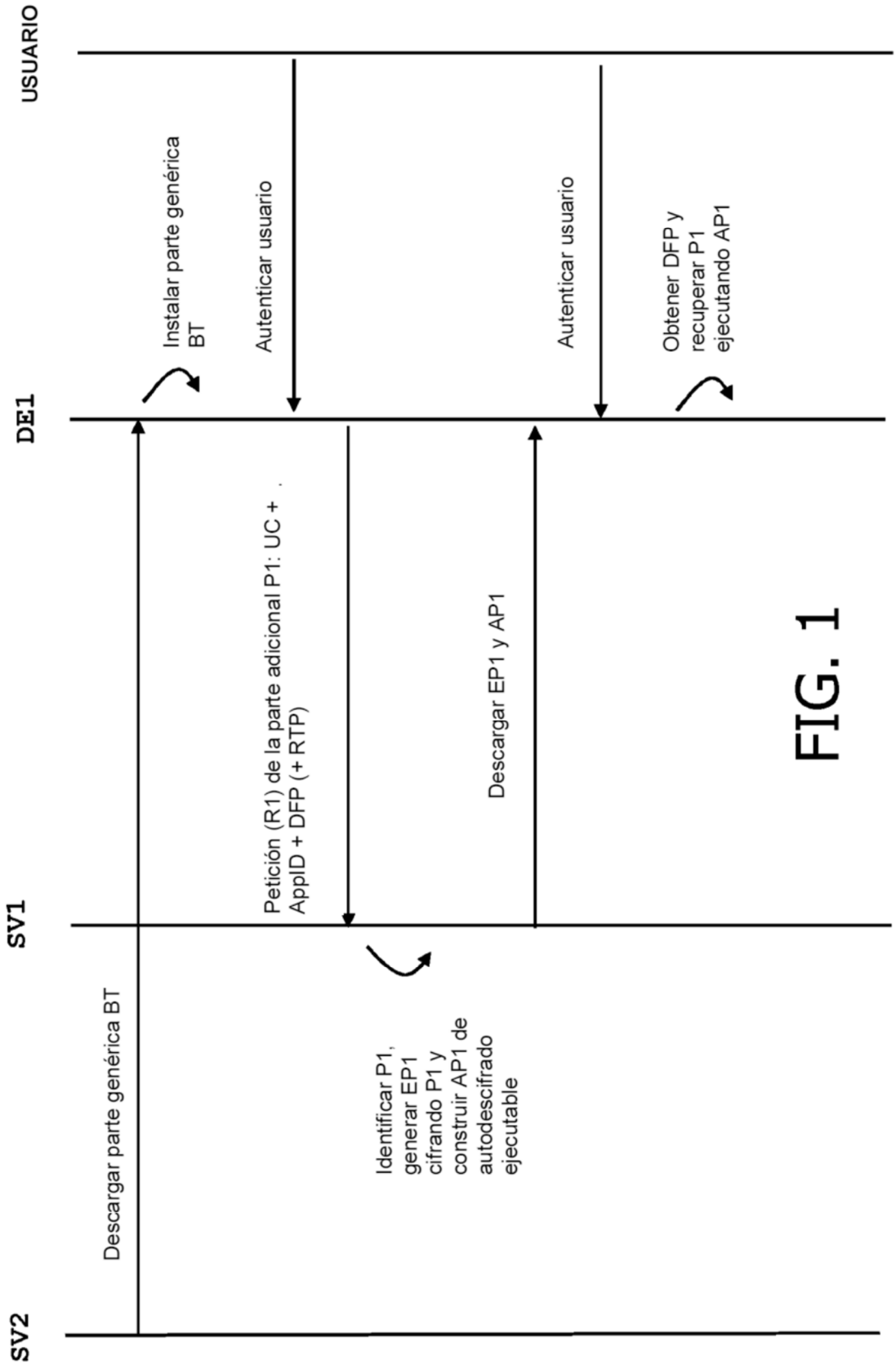
USUARIO
DE1
SV1
SV2
Instalar parte genérica BT
Autenticar usuario
Autenticar usuario
Obtener DFP y recuperar P1 ejecutando AP1
Petición (R1) de la parte adicional P1: UC + AppID + DFP (+ RTP)
Descargar EP1 y AP1
Descargar parte genérica BT
Identificar P1, generar EP1 cifrando P1 y construir AP1 de autodescifrado ejecutable

FIG. 1

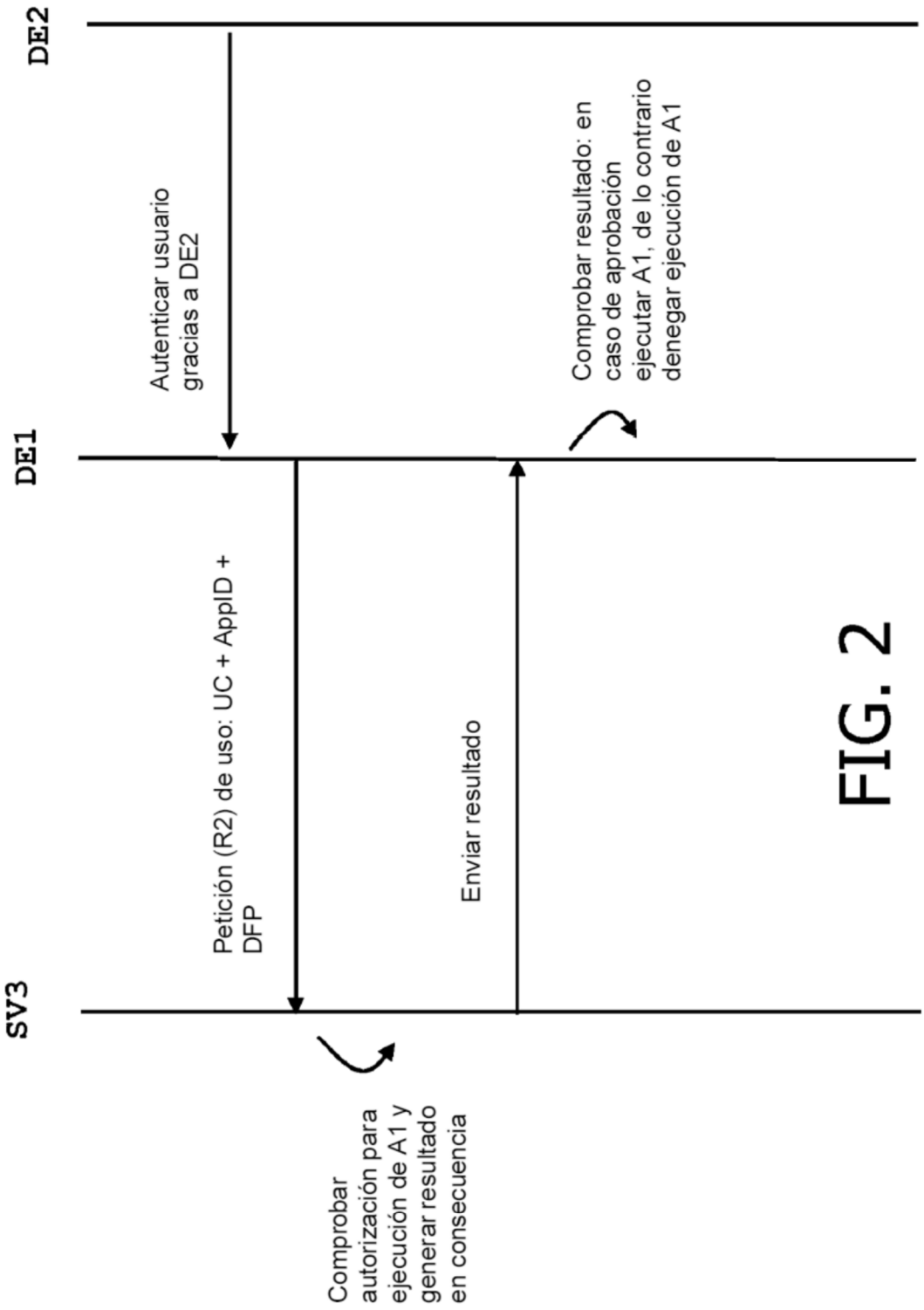
DE2
DE1
SV3
Autenticar usuario gracias a DE2
Comprobar resultado: en caso de aprobación ejecutar A1, de lo contrario denegar ejecución de A1
Petición (R2) de uso: UC + AppID + DFP
Enviar resultado
Comprobar autorización para ejecución de A1 y generar resultado en consecuencia

FIG. 2

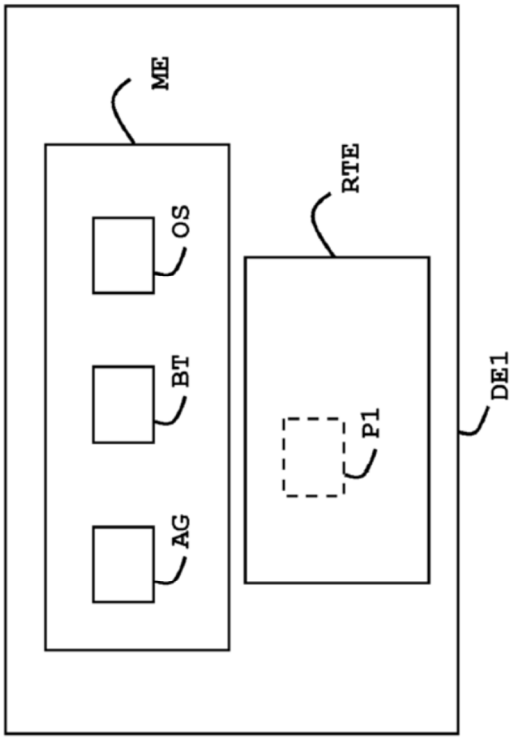


FIG. 4

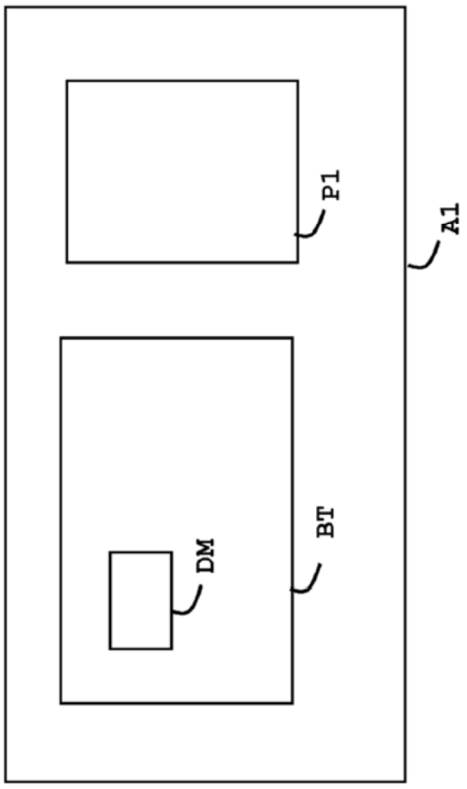


FIG. 3

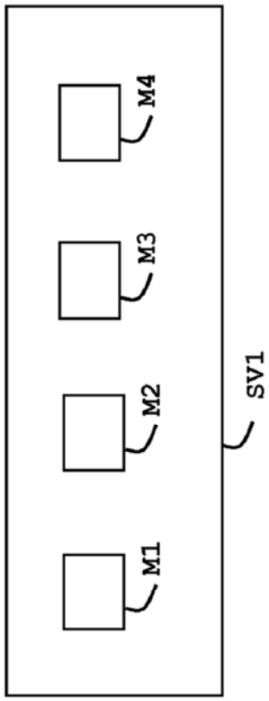


FIG. 5