(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 545 974**

(21) Número de solicitud: 201400211

(51) Int. CI.:

G06F 21/14 (2013.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

17.03.2014

(43) Fecha de publicación de la solicitud:

17.09.2015

(71) Solicitantes:

BANKINTER, S.A. (50.0%)
Paseo de la Castellana, 29
28049 Madrid ES y
SEGLAN, S.L. (50.0%)

(72) Inventor/es:

PÉREZ LAFUENTE, Carlos Alberto;
SAN JOSÉ SÁNCHEZ, Julio y
GARCÍA MURGA, Imanol

(74) Agente/Representante:

LORENTE BERGES, Ana

(54) Título: **Sistema de protección automático y personalizado para aplicaciones móviles**

(57) Resumen:

Se describe un método para generar automáticamente aplicaciones de software de dispositivos móviles, estando cada una personalizada de manera diferente en términos de parámetros de seguridad y/o reglas de ofuscación, utilizando un conjunto de registros de entrada de una primera entidad, conteniendo cada registro de entrada al menos un identificador único utilizado para generar un registro de personalización de salida diferente de otro registro de salida. Una segunda entidad utiliza al menos parte de los datos del registro de salida, una réplica genérica de la aplicación de software de dispositivo móvil y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al menos un identificador único. Un usuario solicita una réplica de la aplicación de software móvil a la primera entidad y una aplicación de software móvil protegida es descargada en un dispositivo móvil del usuario.

ES 2 545 974 A1

DESCRIPCIÓN

Sistema de protección automático y personalizado para aplicaciones móviles

OBJETO DE LA INVENCIÓN

La invención se refiere a un método para personalizar automáticamente, en términos de seguridad, aplicaciones de software de dispositivos móviles. Esta invención también se refiere a un sistema, un servidor, y un dispositivo móvil adecuados para llevar a cabo tal método.

ANTECEDENTES DE LA INVENCIÓN

Las tarjetas inteligentes de microprocesador son comúnmente utilizadas para proteger claves y datos secretos de determinadas aplicaciones por parte de los proveedores de servicios. Consideradas como dispositivos "resistentes a la manipulación", las tarjetas inteligentes se han utilizado para proteger aplicaciones de pagos de bancos, aplicaciones de ticketing de autoridades de transporte, o datos biométricos para control de accesos.

Las tecnologías móviles sin contacto ofrecen una tremenda oportunidad para desplegar aplicaciones y servicios de proveedores de servicios a través de un “contenedor de aplicaciones” con otro factor de forma, y los elementos seguros como las tarjetas SIM, las tarjetas micro-SD o chips embebidos en los teléfonos móviles se han visto durante mucho tiempo como el lugar adecuado para almacenar la parte más sensible de las aplicaciones móviles de los proveedores de servicios.

A pesar del gran potencial de los elementos seguros en términos de capacidades de almacenamiento seguro, diferentes obstáculos - la mayoría de ellos relacionados con los modelos de negocio y la complejidad de los ecosistemas - han limitado sus posibilidades de explotar en áreas tales como los pagos móviles sin contacto.

Para ocupar tal espacio están apareciendo nuevas tecnologías emergentes, algunas de las cuales se basan en nuevos paradigmas de seguridad diferentes del tradicional almacenamiento seguro. En el estado actual de la tecnología, es posible "emular" una tarjeta inteligente mediante software y utilizarla en el contexto de las transacciones sin contacto, utilizando la tecnología denominada "Host Card Emulation" (HCE), actualmente soportada

en los dispositivos Blackberry y Android. Por tanto, es posible llevar a cabo pagos NFC utilizando dicha emulación software de tarjeta inteligente en un teléfono inteligente.

Actualmente existe tecnología para proteger las aplicaciones de software de dispositivos móviles para pagos, transporte, control de acceso, gestión de cupones, banca móvil, operaciones de bolsa a través del móvil, etc., utilizando una combinación de técnicas para obtener una protección de seguridad lógica.

Se supone que los ataques para obtener acceso a, por ejemplo, datos secretos en aplicaciones de software de dispositivos móviles, serán cada vez más severos en el futuro próximo, dado que el incentivo para un atacante de obtener beneficios a partir de los datos almacenados es cada vez mayor. Por ello, se espera que las aplicaciones de software de dispositivos móviles, y en particular las aplicaciones de software para operaciones sin contacto a través del móvil, requerirán la incorporación gradual de las tecnologías de protección de seguridad mencionadas anteriormente.

El principal inconveniente de las tecnologías actuales de protección de aplicaciones de software móviles está relacionado con el hecho de que proporcionan la misma protección para todas las réplicas (por ejemplo, una por usuario y por dispositivo móvil) de una aplicación protegida ejecutable que se suministra a los usuarios finales, de modo que un atacante todavía puede tener el incentivo de burlar la seguridad de una réplica para, utilizando la misma lógica, hacerlo en muchas otras.

Por tanto, puede ser interesante para los proveedores de servicios tener mecanismos disponibles para desplegar una personalización de seguridad diferente para cada usuario que utiliza una determinada aplicación de software móvil.

DESCRIPCIÓN DE LA INVENCIÓN

Por tanto, un primer aspecto de la invención es proporcionar un método de protección personalizado nuevo y automático para aplicaciones de software móviles, en el que diferentes entidades interactúan para proporcionar de manera segura y consistente a cada usuario de una aplicación de software de dispositivo móvil dada (y típicamente para cada uno de sus dispositivos) una solución "resistente a la manipulación" diferente en términos de seguridad lógica, disminuyendo así este sistema de manera drástica los incentivos de un atacante para tratar de obtener datos secretos de incluso el dispositivo móvil de un único

usuario.

Este objetivo se consigue mediante un método para generar automáticamente aplicaciones de software de dispositivos móviles, donde cada una está personalizada de manera diferente en términos de parámetros de seguridad y/o reglas de ofuscación, comprendiendo dicho método las siguientes etapas:

a) Una primera entidad, que es un proveedor de servicios, genera un conjunto de registros de entrada, conteniendo cada registro de entrada al menos un identificador único.

b) Una segunda entidad, que es un personalizador de seguridad de aplicaciones de software de dispositivos móviles, recibe el conjunto de registros de entrada y utiliza el al menos un identificador único incluido en un registro de entrada para generar un registro de personalización de salida, donde este registro de salida es diferente de otro registro de salida generado a partir de otro registro de entrada en términos de parámetros de seguridad y/o reglas de ofuscación para la personalización.

c) La segunda entidad utiliza al menos parte de los datos del registro de salida, una réplica genérica de la aplicación de software de dispositivos móviles y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, siendo esta aplicación de software móvil protegida diferente en términos de parámetros de seguridad y/o reglas de ofuscación de otra aplicación obtenida utilizando al menos parte de otro registro de salida.

d) La segunda entidad envía las aplicaciones de software móvil protegidas a la primera entidad, cada una de ellas asociada a uno o varios identificadores únicos del correspondiente registro de entrada, y la primera entidad las almacena y también almacena la asociación a al menos uno de los identificadores únicos.

e) Un usuario solicita una réplica de la aplicación de software móvil a la primera entidad y una aplicación de software móvil protegida es descargada a un dispositivo móvil del usuario.

Aunque la mayoría de las realizaciones de la descripción de esta invención se refieren a que el conjunto de registros de entrada se envía desde la primera entidad a la segunda entidad comprendidos en uno o varios archivos de entrada, esos registros también se pueden enviar directamente desde una tabla o base de datos de la primera entidad a otra de la segunda entidad, o utilizando otros mecanismos de transmisión.

En una realización particular, la aplicación de software móvil protegida es introducida en un sistema de control de calidad de la segunda entidad, a cargo de determinar si los parámetros de seguridad y/o las reglas de ofuscación han sido adecuadamente

personalizados en la aplicación de software móvil protegida. De este modo, por ejemplo un fallo eléctrico que se produzca durante la personalización de seguridad puede detectarse antes de que la segunda entidad envíe una aplicación de software móvil protegida a la primera entidad.

En una realización particular, la segunda entidad almacena los registros de salida en al menos un archivo de salida y almacena el al menos un archivo de salida en sus sistemas.

En otra realización particular, el al menos un archivo de salida es enviado por la segunda entidad a la primera entidad, y la primera entidad lo almacena en sus sistemas. De este modo, la primera entidad tiene disponible en sus sistemas la información acerca de la protección de seguridad que al menos parcialmente aplica a cada una de las réplicas de una aplicación de software móvil dada.

En una realización particular, la primera entidad asigna el al menos un identificador único del registro de entrada a un usuario particular antes de enviar el conjunto de registros de entrada a la segunda entidad, de modo que la aplicación de software móvil protegida ya está asignada a un usuario dado cuando es recibida por la primera entidad desde la segunda entidad.

En otra realización particular, se asigna la misma aplicación de software móvil protegida a todos los dispositivos móviles de un usuario. De ese modo, la protección de la aplicación de software móvil se aplica por cada usuario, y no por cada dispositivo, lo que sigue dificultando suficientemente a un atacante que pueda atacar muchas aplicaciones de software móvil protegidas si ha tenido éxito burlando la seguridad de una.

En otra realización particular, se asigna una aplicación de software móvil protegida diferente a cada uno de los dispositivos móviles del usuario. Ventajosamente, este método proporciona una protección por cada usuario y por cada dispositivo a una aplicación de software móvil dada.

En una realización particular, la primera entidad asigna el al menos un identificador único del registro de entrada, y la aplicación de software móvil protegida, a un usuario particular después de haber recibido la correspondiente aplicación de software móvil protegida desde la segunda entidad y después de que el usuario se haya registrado con éxito en un servicio del proveedor de servicios utilizando la aplicación de software móvil protegida. De ese

modo, la asignación se produce como resultado del interés del usuario en recibir servicios a través de la aplicación de software móvil protegida.

En otra realización particular, la primera entidad asigna el al menos un identificador único del registro de entrada, y la aplicación de software móvil protegida, a un dispositivo móvil particular de un usuario después haber recibido la correspondiente aplicación de software móvil protegida desde la segunda entidad y después de que el usuario se haya registrado con éxito en un servicio del proveedor de servicios utilizando la aplicación de software móvil protegida. De modo que en este caso la asignación también se lleva a cabo como resultado del interés del usuario en recibir servicios a través de la aplicación de software móvil protegida, pero ello se hace por cada dispositivo móvil del usuario.

En una realización particular, algunos de los parámetros de seguridad personalizados en la aplicación de software móvil protegida son enviados a la primera entidad en el contexto de una conexión en línea desde la aplicación de software móvil protegida, y la primera entidad valida los parámetros de seguridad. Ventajosamente, la primera entidad es capaz de determinar si esos parámetros son válidos y, en caso contrario, deshabilitar la aplicación de software móvil protegida en el sistema de la primera entidad.

En una realización particular, la aplicación de software móvil protegida es descargada en el dispositivo móvil del usuario como resultado de otra aplicación, que ha sido instalada previamente en dicho dispositivo móvil del usuario, que se dirige a una dirección remota particular, y al menos uno de los servicios en línea no está disponible para la aplicación de software móvil protegida si un proceso de registro con éxito que requiere que el usuario introduzca un código de activación en la aplicación de software móvil protegida no ha sido completado dentro de un período de tiempo dado después de que la aplicación de software móvil protegida haya sido descargada en el dispositivo móvil del usuario, estando definido dicho período de tiempo por la primera entidad. La otra aplicación referida puede ser, por ejemplo, una aplicación "lanzador" (capaz de enlazar, por ejemplo, con una dirección web particular) o un buscador del dispositivo móvil.

Una primera ventaja de esta realización es que la aplicación de software móvil protegida sólo puede ser descargada desde una(s) direccion(es) remota(s) definida(s) por la primera entidad. En algunas realizaciones, el usuario debe autenticarse y firmar la solicitud remota para conseguir que la aplicación móvil protegida sea descargada en el dispositivo móvil.

Una segunda ventaja de esta realización es que existe un período de tiempo limitado para que el usuario complete el proceso de registro, y por tanto existe un período de tiempo limitado para que un hacker pueda atacar la aplicación antes de que termine el proceso de registro. Si se supera dicho período de tiempo, uno o varios servicios online no estarán disponibles mediante la aplicación de software móvil protegida. Esta medida será de gran interés para un proveedor de servicios con relación, por ejemplo, a servicios en línea donde están implicados pagos (por ejemplo, pagos NFC o e-commerce realizados a través de la aplicación de software móvil protegida), que pueden ser restringidos si el registro se lleva a cabo fuera de la ventana temporal definida. En una implementación particular, si se excede el período de tiempo la primera entidad deshabilita la aplicación de software móvil protegida en sus sistemas de modo que no habrá servicios en línea disponibles a través de la aplicación móvil.

En una realización particular, la aplicación de software móvil protegida se utiliza para proporcionar un conjunto de servicios en línea al usuario y al menos uno de esos servicios en línea no está disponible para la aplicación de software móvil protegida hasta que ha sido registrada en los sistemas de la primera entidad mediante la introducción por parte del usuario de un código de activación en el dispositivo móvil y la selección de un PIN, requiriéndose el PIN para tener acceso al al menos un servicio en línea.

En una implementación particular, el usuario selecciona el PIN introduciéndolo en el dispositivo móvil, como parte del proceso de registro de la aplicación de software móvil protegida.

De modo que en esta realización el uso de la aplicación de software móvil protegida puede restringirse hasta que el usuario lleva a cabo con éxito un proceso de registro seguro (por ejemplo, el código de activación se obtiene después de que el usuario se haya autenticado en la página web del proveedor de servicios y haya firmado la solicitud, y tiene un tiempo de validez limitado).

En otra realización particular, la aplicación de software móvil protegida se utiliza para proporcionar servicios de pagos móviles en línea sin contacto al usuario y dichos servicios de pagos no están disponibles para la aplicación de software móvil protegida hasta que la primera entidad descarga a la aplicación de software móvil protegida al menos una parte de al menos una credencial para su uso en los servicios de pagos móviles en línea sin contacto. En un ejemplo particular, la al menos una parte de la al menos una credencial es

descargada durante el proceso de registro de la aplicación de software móvil protegida, después el usuario introduce un código de activación en el dispositivo móvil y selecciona un PIN, requiriéndose el PIN para realizar pagos móviles en línea sin contacto. En otro ejemplo, se descarga después del proceso de registro, como resultado de la inserción del PIN por parte del usuario en la aplicación móvil y de que la primera entidad verifique que es correcto.

De modo que, en esta realización, el uso de la aplicación de software móvil protegida puede también estar restringido hasta que al menos una parte de al menos una credencial está disponible en la aplicación de pagos móviles protegida (y la recepción de dicha al menos parte de al menos una credencial en la aplicación de software móvil protegida típicamente requiere que el usuario inserte un código de activación - por ejemplo, obtenido a través de otro canal – y/o inserte un PIN - que será verificado por la primera entidad -).

En una realización particular, al menos un dato del registro de personalización de salida no se utilizó para generar la aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, y al menos parte de esos datos son enviados a la primera entidad, y la primera entidad re-personaliza al menos parcialmente la aplicación de software móvil protegida, en términos de al menos parte de los parámetros de seguridad y/o las reglas de ofuscación, utilizando al menos parte de esos datos. De modo que al utilizar esta realización los parámetros de seguridad y/o las reglas de ofuscación pueden ser renovadas en la aplicación de software móvil protegida cuando la personalización de seguridad actual caduque o esté cerca de caducar.

En una realización particular, un nuevo registro de personalización de salida, asociado al al menos un identificador único, es generado por la segunda entidad durante el ciclo de vida de una aplicación de software móvil protegida determinada, y al menos parte de este nuevo registro de salida es enviado a la primera entidad, y la primera entidad re-personaliza al menos parcialmente la aplicación de software móvil protegida, en términos de al menos parte de los parámetros de seguridad y/o reglas de ofuscación, utilizando datos incluidos en el nuevo registro de salida. De modo que si los datos de personalización de seguridad del registro de salida anterior se han consumido o han caducado, la segunda entidad puede generar nuevos datos y enviarlos a la primera entidad para re-personalizar la aplicación de software móvil protegida en términos de parámetros de seguridad y/o reglas de ofuscación.

En una realización particular, uno o varios procesos que pertenecen al dominio de la primera entidad son llevados a cabo por la segunda entidad, o por un tercero de confianza, en

nombre de la primera entidad. En un ejemplo particular, la solicitud de un usuario de una réplica de la aplicación de software móvil es recibida por la segunda entidad, que descarga una aplicación de software móvil protegida y la asigna a un dispositivo móvil dado de un usuario, en nombre de la primera entidad. En otro ejemplo, la asignación es llevada a cabo por un tercero de confianza, en nombre de la primera entidad, después de que el usuario se haya registrado con éxito en un servicio del proveedor de servicios utilizando la aplicación de software móvil protegida.

En una realización particular, uno o varios procesos de la segunda entidad son proporcionados por la primera entidad, o por un tercero de confianza, en nombre de la primera entidad. En un ejemplo particular, la primera entidad es el personalizador de seguridad de aplicaciones de software de dispositivos móviles.

Un segundo aspecto de la invención está dirigido a un sistema para generar automáticamente aplicaciones de software de dispositivos móviles, donde cada una está personalizada de manera diferente en términos de parámetros de seguridad y/o reglas de ofuscación, comprendiendo dicho sistema:

- medios de generación que permiten a una primera entidad generar un conjunto de registros de entrada, conteniendo cada registro de entrada al menos un identificador único;
- medios de personalización de seguridad que permiten a una segunda entidad personalizar aplicaciones de software para dispositivos móviles, después de recibir el conjunto de registros de entrada, utilizando el al menos un identificador único incluido en un registro de entrada para generar un registro de personalización de salida;
- medios de transmisión para que la segunda entidad envíe las aplicaciones de software móvil protegidas a la primera entidad, estando cada una asociada a uno o varios identificadores únicos del correspondiente registro de entrada;
- medios de almacenamiento para que la primera entidad almacene las aplicaciones de software móviles protegidas y la asociación con al menos uno de los identificadores únicos;
- medios de interfaz de usuario para permitir al usuario solicitar una réplica de la aplicación de software móvil a la primera entidad; y
- medios de transmisión para que una aplicación de software móvil protegida sea descargada por la primera entidad a un dispositivo móvil del usuario,

donde el registro de salida es diferente de otro registro de salida, generado a partir de otro

registro de entrada, en términos de parámetros de seguridad y/o reglas de ofuscación para la personalización, y los datos del registro de salida serán al menos parcialmente introducidos en una réplica genérica de una aplicación de software para dispositivos móviles, y la segunda entidad utiliza la al menos parte del registro de salida, la réplica genérica de la aplicación de software para dispositivos móviles y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, siendo esta aplicación de software móvil protegida diferente en términos de parámetros de seguridad y/o reglas de ofuscación que otra obtenida utilizando al menos parte de otro registro de salida.

El documento de patente US 2013/0042300 describe un método para proporcionar un nivel de seguridad dado a una aplicación en un dispositivo final, pero dicho método sólo se aplica después de que la aplicación ha sido descargada en dicho dispositivo final, ya que la solicitud de un nuevo nivel de seguridad de hecho se lleva a cabo desde la propia aplicación. Por el contrario, en el contexto de la invención, se proporciona una protección de seguridad a la aplicación de software móvil antes que la aplicación sea descargada en el dispositivo móvil, y por tanto el proceso de seguridad es gestionado enteramente desde un nivel central y la seguridad es aplicada desde ese nivel, antes de la descarga de la aplicación. Ventajosamente, en comparación con el documento US 2013/0042300, la invención permite aplicar la protección de seguridad a priori, y por tanto la aplicación que se descarga al dispositivo móvil ya está protegida.

Además, el documento US 2013/0042300 se refiere a un lugar central que asigna, como resultado de una solicitud de la aplicación del dispositivo final de usuario, una configuración de seguridad predefinida de entre un conjunto limitado de configuraciones para dicho tipo de dispositivo final. Por tanto, el documento US 2013/0042300 se refiere a un conjunto de posibles configuraciones de seguridad de la aplicación, y no a una personalización de la seguridad de la aplicación diferente por cada usuario. No se sugiere en el documento US 2013/0042300 la posibilidad de aplicar una personalización de seguridad de la aplicación diferente por cada usuario, o por cada dispositivo de usuario. Por el contrario, la invención se refiere al usuario que solicita una réplica de la aplicación de software móvil, y una aplicación de software móvil protegida que es diferente en términos de parámetros de seguridad y/o reglas de ofuscación de cualquier otra, es descargada en el dispositivo móvil del usuario. Por tanto, la invención proporciona mecanismos para suministrar una protección de seguridad a la aplicación que es diferente por cada usuario (evitando así un ataque masivo a la aplicación de software móvil).

Por último, aunque no menos importante, está el hecho de que el documento US 2013/0042300 indica que una o varias funciones de la aplicación están configuradas sobre la base de la configuración de seguridad aplicada (por ejemplo, como resultado de la nueva configuración de seguridad se requiere ahora un PIN para acceder a una característica determinada). De modo que en el documento US 2013/0042300 la funcionalidad de la aplicación se ve directamente afectada por la nueva configuración de seguridad. Por el contrario, en el contexto de la invención, la protección aplicada no afecta a la funcionalidad de la aplicación, sino que simplemente proporciona una seguridad por cada usuario, basada en técnicas de ofuscación, a la aplicación de software móvil. En otras palabras, la protección no tiene ningún impacto en la funcionalidad proporcionada por la aplicación al usuario final.

BREVE DESCRIPCIÓN DE LAS FIGURAS

En la siguiente descripción detallada de algunas realizaciones, aparecerán otras características y ventajas de la invención, realizándose cada descripción con referencia a las siguientes figuras:

La Fig. 1 muestra un diagrama esquemático que ilustra varias realizaciones de un sistema de protección automático y personalizado para aplicaciones móviles de acuerdo con la invención.

La Fig. 2 un diagrama esquemático que ilustra otras realizaciones de un sistema de protección automático y personalizado para aplicaciones móviles de acuerdo con la invención.

Las Figs. 3a-3c muestran un diagrama esquemático de parte de diversas realizaciones de acuerdo con la invención.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

La Figura 1 es un diagrama esquemático que ilustra una realización de un sistema de protección automático y personalizado para aplicaciones móviles de acuerdo con la invención.

La Figura muestra el sistema (100) de una primera entidad, que es un proveedor de

servicios, y el sistema (200) de una segunda entidad, que es un personalizador de seguridad de aplicaciones de software móviles. Ambos están preparados para ejecutar un método de acuerdo con la invención.

En la etapa (1), la primera entidad genera un archivo de entrada que comprende un conjunto de registros de entrada, conteniendo cada registro de entrada al menos un identificador único. La Figura 1 ilustra un ejemplo particular donde hay un solo identificador único (i) asociado a cada registro de entrada (i). Este identificador único puede ser un código único de transacción asociado al registro de entrada. Todavía en la etapa (1), el archivo de entrada es almacenado en las bases de datos (BBDD) de la primera entidad relativas a la protección de seguridad de aplicaciones de software móviles, conforme a la invención.

En la etapa (2), la primera entidad envía el archivo de entrada, y la segunda entidad lo recibe.

En la etapa (3), la segunda entidad genera un archivo de personalización de salida a partir de los datos incluidos en el archivo de entrada, generando un registro de salida en el archivo de salida por cada uno de los registros de entrada en el archivo de entrada. El identificador único (i) del registro de entrada (i) se utiliza para generar el registro de salida (i). En un ejemplo particular, el identificador único (i) es simplemente parte del registro de salida (i); en otro ejemplo, el identificador único (i) también se utiliza para calcular datos de personalización del registro de salida (i). Todavía en la etapa (3), tanto el archivo de entrada como el archivo de personalización de salida son almacenados en las BBDD de la segunda entidad relativas a la protección de seguridad de aplicaciones de software móviles, de acuerdo con la invención.

De modo que en esta realización, la segunda entidad almacena los registros de salida en al menos un archivo de salida, y almacena el al menos un archivo de salida en sus sistemas.

Los datos de personalización de un registro de salida (i) dado son calculados en la etapa (3) para que sean diferentes de los datos de personalización de otro registro de salida (j). En una implementación particular, esto se consigue utilizando el identificador único (i) como entrada para el cálculo de los datos de personalización del registro de salida (i) y el identificador único (j) como entrada para el cálculo de los datos de personalización del registro de salida (j).

En el contexto de la invención, cada registro de salida contiene datos que se utilizarán posteriormente, al menos parcialmente, para proteger una aplicación de software móvil. En esta realización, tales datos se utilizarían como parámetros de seguridad, y también para definir reglas de ofuscación para proteger una aplicación de software móvil. Para conseguirlo, los datos serán introducidos en una réplica genérica de una aplicación de software de teléfonos móviles dada.

De modo que en esta realización una segunda entidad, que es un personalizador de seguridad de aplicaciones de software de dispositivos móviles, recibe el conjunto de registros de entrada y utiliza el al menos un identificador único incluido en un registro de entrada para generar un registro de personalización de salida, donde este registro de salida es diferente de otro registro de salida generado a partir de otro registro de entrada en términos de parámetros de seguridad y/o reglas de ofuscación para la personalización, y los datos del registro de salida serán al menos parcialmente introducidos en una réplica genérica de una aplicación de software para dispositivos móviles.

En la etapa (4), la segunda entidad utiliza los datos de personalización de seguridad en el registro de salida 1 como datos para ser introducidos a un software de ofuscación, capaz de ofuscar una réplica genérica de la aplicación de software móvil utilizando los referidos datos de personalización del registro de salida 1. El resultado del proceso de ofuscación es una aplicación de software móvil protegida que está asociada al registro de salida 1 y al identificador único 1 correspondiente, estando relacionada la protección con parámetros de seguridad y reglas de ofuscación personalizados. El proceso se repite para cada uno de los registros de salida del archivo de personalización de salida, de modo que se generan N aplicaciones de software móvil protegidas, cada una de ellas asociada a su correspondiente registro de salida e identificador único. Todavía en la etapa (4), las N aplicaciones de software móvil protegidas y la asociación de cada una con el registro de salida correspondiente y el identificador único son almacenadas en las BBDD de la segunda entidad relativa a protección de seguridad de aplicaciones de software móvil, de acuerdo con la invención.

Como se ha descrito anteriormente, los datos de personalización de un registro de salida (i) dado se calculan de modo que son diferentes que los datos de personalización de otro registro de salida (j) .De ese modo, la aplicación de software móvil protegida asociada al registro de salida (i) y al identificador único (i) correspondiente será diferente, en términos de parámetros de seguridad y/o reglas de ofuscación personalizados, que la aplicación de

software móvil protegida asociada al registro de salida (j) y identificador único (j) correspondiente.

De modo que en esta realización, la segunda entidad utiliza al menos parte de los datos del registro de salida, una réplica genérica de la aplicación de software de dispositivos móviles, y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, siendo esta aplicación de software móvil protegida diferente en términos de parámetros de seguridad y/o reglas de ofuscación de otra aplicación obtenida utilizando al menos parte de otro registro de salida.

En la etapa (5), la segunda entidad envía las aplicaciones de software móviles protegidas a la primera entidad, cada una de ellas asociada al correspondiente identificador único del registro de entrada correspondiente, y la primera entidad las recibe y almacena en las BBDD de la primera entidad relativas a la protección de seguridad de aplicaciones de software móviles, de acuerdo con la invención.

De modo que la segunda entidad envía las aplicaciones de software móvil protegidas a la primera entidad, cada una de ellas asociada a uno o varios identificadores únicos del correspondiente registro de entrada, y la primera entidad las almacena y también almacena la asociación a al menos uno de los identificadores únicos.

En una implementación particular, la segunda entidad también envía a la primera entidad en la etapa (5) el archivo de personalización de salida. De modo que en esta implementación particular, el al menos un archivo de salida es enviado por la segunda entidad a la primera entidad, y la primera entidad lo almacena en sus sistemas.

En esta realización, la primera entidad asigna el identificador único de cada registro de entrada a un usuario particular en la etapa (1), antes de enviar el archivo de entrada a la segunda entidad, de modo que las BBDD de la primera entidad relacionadas con la protección de seguridad de aplicaciones de software móvil tendrían esta asignación almacenada desde la etapa (1).

De modo que en esta realización, la primera entidad asigna el al menos un identificador único del registro de entrada a un usuario particular antes de enviar el conjunto de registros de entrada a la segunda entidad, de modo que la aplicación de software móvil protegida ya está asignada a un usuario dado cuando es recibida por la primera entidad desde la

segunda entidad. Y la misma aplicación de software móvil protegida será asignada a todos los dispositivos móviles del usuario.

En la etapa (6), un usuario (300) solicita una réplica de la aplicación de software móvil a la primera entidad. En esta realización, el usuario ha descargado previamente en su dispositivo móvil (400) una aplicación de instalación desde una tienda de aplicaciones, y envía una solicitud para recibir una réplica de la aplicación de software móvil utilizando la aplicación de instalación en el dispositivo móvil. La solicitud es enviada al servidor de la primera entidad asociado a las aplicaciones de software móvil protegidas. La primera entidad busca en las BBDD la aplicación de software móvil protegida asignada al usuario en la etapa (1) y el servidor de aplicaciones la descarga al dispositivo móvil del usuario.

De modo que en esta realización, un usuario solicita una réplica de la aplicación de software móvil a la primera entidad y una aplicación de software móvil protegida es descargada a un dispositivo móvil del usuario.

La Figura 1 también ilustra otra realización de acuerdo con la invención donde la asignación del identificador único de cada registro de entrada a un usuario particular no se lleva a cabo en la etapa (1), sino después de que el usuario se haya registrado con éxito en al menos una parte de los servicios del proveedor de servicios que se relacionan con el uso de la aplicación de software móvil protegida.

En esta realización, una vez la aplicación de software móvil protegida ha sido descargada en la etapa (6), en la etapa (7) el usuario obtiene un código de activación a través de la página web del proveedor de servicios, después de autenticarse con éxito y firmar la transacción.

Como resultado de la inserción del código de activación en la aplicación de software móvil protegida por parte del usuario, la aplicación inicia (por ejemplo, vía https) un proceso de registro seguro en los referidos servicios a través del servidor de la primera entidad asociado a las aplicaciones de software móvil protegidas, incluyendo el proceso de envío del código de activación desde la aplicación de software móvil protegida al servidor de la primera entidad, y una vez el registro ha sido completado con éxito, la primera entidad asigna, en las BBDD para las aplicaciones de software móvil protegidas, la aplicación de software móvil protegida al usuario. Por tanto, la asignación se lleva a cabo como resultado del interés del usuario en recibir servicios a través de la aplicación de software móvil protegida.

De modo que en esta realización, la primera entidad asigna el al menos un identificador único del registro de entrada, y la aplicación de software móvil protegida, a un usuario particular después de haber recibido la correspondiente aplicación de software móvil protegida de la segunda entidad y después de que el usuario se haya registrado con éxito en un servicio del proveedor de servicios utilizando la aplicación de software móvil protegida.

La Figura 1 también ilustra otra realización de acuerdo con la invención donde la asignación del identificador único de cada registro de entrada a un usuario particular no se realiza en la etapa (1), sino después de que el usuario se haya registrado con éxito en al menos parte de los servicios del proveedor de servicios relacionados con el uso de la aplicación de software móvil protegida.

En esta realización, una vez la aplicación de software móvil protegida ha sido descargada en la etapa (6), en la etapa (7) el usuario obtiene un código de activación a través de la página web del proveedor de servicios, después de autenticarse con éxito y firmar la transacción.

Como resultado de la inserción del código de activación por parte de usuario en la aplicación de software móvil protegida, la aplicación inicia (por ejemplo, a través de https) un proceso de registro seguro a los servicios referidos a través del servidor de la primera entidad asociado a las aplicaciones de software móvil protegidas, incluyendo el proceso enviar el código de activación y al menos un identificador único del dispositivo móvil desde la aplicación de software móvil protegida al servidor de la primera entidad, y una vez se ha completado con éxito el registro, la primera entidad asigna, en las BBDD para las aplicaciones de software móvil protegidas, la aplicación de software móvil protegida al dispositivo móvil del usuario. Por tanto, en este caso la asignación se lleva a cabo también como resultado del interés del usuario en recibir servicios a través de la aplicación de software móvil protegida, pero se hace en base a cada dispositivo móvil del usuario.

De modo que en esta realización, la primera entidad asigna el al menos un identificador único del registro de entrada, y la aplicación de software móvil protegida, a un dispositivo móvil particular de un usuario después de haber recibido la correspondiente aplicación de software móvil protegida de la segunda entidad y después de que el usuario se haya registrado con éxito en un servicio del proveedor de servicios utilizando la aplicación de software móvil protegida.

Considerando que en esta realización la asignación de la aplicación de software móvil

protegida es por cada dispositivo del usuario, si el usuario solicitase más tarde la descarga de una réplica de la aplicación de software móvil a otro de sus dispositivos móviles, la aplicación de software móvil protegida descargada sería diferente, en términos de parámetros de seguridad y/o reglas de ofuscación, que cualquier otra descargada previamente en otro dispositivo de ese usuario.

Por tanto, en esta realización se asigna una aplicación de software móvil protegida diferente a cada uno de los dispositivos móviles del usuario.

Las primeras tres realizaciones anteriores pueden ser utilizadas para proteger de manera fiable una pluralidad de aplicaciones de software móviles, bien para cada usuario, o bien para cada dispositivo móvil del usuario. Las realizaciones se podrían aplicar a aplicaciones de bancos para operaciones en bolsa, aplicaciones de mensajería multimedia de empresas de telecomunicaciones o vendedores de teléfonos inteligentes, aplicaciones relativas a la gestión de cupones de comerciantes, aplicaciones de operadores de transporte que ofrecen descubrimiento de rutas a sus usuarios, o bien aplicaciones móviles de medios sociales.

En el contexto de cualquiera de esas realizaciones de ejemplo, una réplica protegida de una aplicación de software móvil en un dispositivo móvil de un usuario es siempre diferente de otra réplica protegida de la misma aplicación de software móvil en el dispositivo móvil de otro usuario, en términos de parámetros de seguridad y/o reglas de ofuscación.

De modo que implementar cualquiera de esas realizaciones implica que, en lo que respecta a ciertos tipos de ataques, un hacker que intente obtener un control no autorizado de una primera réplica de la aplicación de software móvil protegida en el dispositivo móvil de un usuario tendría que dedicar el mismo esfuerzo para obtener un control no autorizado de otra réplica de la aplicación de software móvil protegida en el dispositivo móvil de otro usuario, y así sucesivamente, de modo que el incentivo para un ataque masivo se reduce drásticamente. Como ejemplo particular, si un atacante es capaz de obtener un dato secreto ofuscado en el código de una réplica protegida de una aplicación de software móvil en el dispositivo de un usuario, como resultado de haber obtenido la regla de ofuscación para esa réplica de la aplicación y ese dato secreto, deberá dedicar de nuevo el mismo tiempo para obtener el dato secreto equivalente ofuscado en el código de otra réplica protegida de la misma aplicación de software móvil en el dispositivo móvil de otro usuario.

Además de la protección anterior, también es posible añadir protección adicional [por

usuario / por dispositivo de usuario] a las aplicaciones de software móvil, en términos de si dar o no a esas aplicaciones el derecho de acceder a ciertos servicios en línea. Dar a la aplicación de software móvil protegida acceso a ciertos servicios en línea sólo como resultado de la selección con éxito de un PIN por parte del usuario a través de la aplicación, o de la finalización de un proceso de registro de la aplicación dentro de un período de tiempo predefinido limitado, o de la obtención de ciertas credenciales que se requieren para servicios en línea, proporciona al proveedor de servicios una protección de seguridad adicional y un mayor control. Este nivel de protección adicional puede ser adecuado para aplicaciones de software móvil protegidas que gestionen servicios de pagos o ticketing.

La Figura 1 también ilustra otra realización de acuerdo con la invención donde el usuario ha descargado en su dispositivo móvil, antes de la etapa (6), una aplicación de instalación desde una tienda de aplicaciones. Dentro de esta realización, el usuario tendrá un período de tiempo limitado para registrar su aplicación de software móvil protegida.

En la etapa (6), el usuario solicita una réplica de la aplicación de software móvil a la primera entidad utilizando la aplicación de instalación en el dispositivo móvil. Al igual que en algunas de las realizaciones anteriores, en esta realización de ejemplo la asignación del al menos un identificador único del registro de entrada, y de la aplicación de software móvil protegida, al dispositivo móvil de un usuario particular se lleva a cabo después de que el usuario se haya registrado con éxito en al menos parte de los servicios del proveedor de servicios que son relativos al uso de la aplicación de software móvil protegida.

En esta realización, una vez la aplicación de software móvil protegida ha sido descargada en la etapa (6), en la etapa (7) el usuario obtiene un código de activación a través de la página web del proveedor de servicios, después de autenticarse con éxito y firmar la transacción.

Como resultado de la inserción por el usuario del código de activación en la aplicación de software móvil protegida, la aplicación inicia (por ejemplo, vía https) un proceso de registro seguro en los servicios referidos a través del servidor de la primera entidad asociado a las aplicaciones de software móvil protegidas, incluyendo el proceso enviar el código de activación y al menos un identificador único de dispositivo móvil desde la aplicación de software móvil protegida al servidor de la primera entidad, y una vez que el registro se ha completado con éxito, la primera entidad asigna, en las BBDD para las aplicaciones de software móvil protegidas, la aplicación de software móvil protegida al dispositivo móvil del usuario.

En esta realización, hay un período de tiempo predefinido y limitado después de que la aplicación de software móvil protegida ha sido descargada en el dispositivo móvil del usuario para terminar el proceso de registro; si se supera el período de tiempo predefinido, entonces la primera entidad deshabilitará ciertos servicios en línea para la aplicación de software móvil protegida.

De modo que en esta realización, la aplicación de software móvil protegida es descargada en el dispositivo móvil del usuario como el resultado de otra aplicación, que ha sido instalada previamente en dicho dispositivo móvil del usuario, que se dirige a una dirección remota particular, y al menos uno de los servicios en línea no está disponible para la aplicación de software móvil protegida si un proceso de registro con éxito que requiere que el usuario introduzca un código de activación en la aplicación de software móvil protegida no ha sido completado dentro de un período de tiempo dado después de que la aplicación de software móvil protegida haya sido descargada en el dispositivo móvil del usuario, estando definido dicho período de tiempo por la primera entidad.

En esta realización, la aplicación de software móvil protegida sólo puede ser descargada desde una(s) direccion(es) remota(s) definida(s) por la primera entidad.

Ventajosamente, la primera entidad puede utilizar al menos parte de los parámetros de seguridad, ofuscados en la aplicación de software móvil, para verificar la autenticidad de la aplicación durante el proceso de registro.

Y existe un período de tiempo limitado para que el usuario complete el proceso de registro, por tanto existe un tiempo limitado para que un hacker ataque la aplicación antes de que el proceso de registro termine. Como un ejemplo particular, un proveedor de servicios bancarios puede bloquear los pagos móviles NFC o e-commerce en línea en el servidor de pagos cuando éstos son realizados a través de una aplicación de software móvil protegida que no se registró dentro del período de tiempo predefinido.

La Figura 2 ilustra otra realización de acuerdo con la invención. Para una mejor comprensión, esta realización se describe con referencia al documento PCT/EP2013/066540, que pertenece al mismo solicitante que la presente solicitud. El documento PCT/EP2013/066540 se refiere a un método para habilitar pagos/ticketing sin contacto a través de una aplicación de teléfono móvil. En particular, la figura 2.b del

documento PCT/EP2013/066540 muestra un sistema de pagos de ejemplo para habilitar pagos móviles sin contacto a través de una aplicación de teléfono móvil donde:

- En la etapa (5) se genera el código de activación. En la etapa (7), el usuario inserta el código de activación en la aplicación de pagos del teléfono móvil y en la etapa (8) el teléfono móvil envía al módulo servidor de pagos, por ejemplo vía https, el [código de activación y el hash (número de identificación del dispositivo móvil & código de activación)].

- En la etapa (10), la tarjeta "A" es pre-personalizada en la aplicación del teléfono móvil. Cuando la etapa (10) termina, el usuario ya está registrado en el sistema de la invención.

- En la etapa (11), se solicita al usuario que seleccione un Número de Identificación Personal (PIN, Personal Identification Number) para los servicios de pagos móviles sin contacto. El valor del PIN no se almacena en la aplicación de pagos del teléfono móvil, sino que se envía de manera segura en la etapa (12) al módulo servidor de pagos, junto con una Contraseña de Único Uso (OTP, One Time Password) calculada utilizando el valor del PIN (y junto con el Código de Activación y el hash (AC&ID)). En la etapa (13), el PIN es almacenado en la base de datos del módulo servidor de pagos, junto con las claves y los parámetros para calcular un resultado OTP basado en el PIN.

- Todavía en la etapa (13), el módulo servidor de pagos calcula un resultado OTP utilizando el PIN almacenado del usuario y las claves y parámetros OTP, y compara el resultado con el recibido de la aplicación de pagos del teléfono móvil. Si la validación tiene éxito, entonces se pueden enviar credenciales de pago a la aplicación de pagos del teléfono móvil. De modo que el módulo servidor de pagos envía credenciales al teléfono móvil registrado del usuario después de la validación con éxito de una Contraseña de Único Uso (OTP) recibida desde la aplicación de pagos del teléfono móvil.

- En la etapa (14), se envía un primer conjunto de credenciales (por ejemplo, credenciales desde i=1 hasta i=j, j<n) a la aplicación de pagos del teléfono móvil; el teléfono móvil del usuario recibe las credenciales y las almacena para su uso en comercios equipados con Terminales Punto de Venta sin contacto.

- El usuario registrado puede en la etapa (15) utilizar el teléfono móvil para pagar en comercios equipados con Terminales Punto de Venta sin contactos. En la etapa (15), el usuario debe insertar su código PIN en la aplicación de pagos del teléfono móvil antes de tratar de pagar en el Terminal Punto de Venta sin contactos 4000.

De modo que en el ejemplo anterior de sistema de pagos de PCT/EP2013/066540, el proceso de registro de la aplicación del teléfono móvil comienza en la etapa (5) (cuando se genera el código de activación) y termina en la etapa (14) (después de que el usuario haya seleccionado un PIN para pagos móviles sin contacto y un primer conjunto de credenciales para pagos móviles sin contacto haya sido almacenado en la aplicación de pagos del teléfono móvil).

En el contexto de la presente invención para proporcionar una protección automática y personalizada para aplicaciones de software móviles, y con relación al ejemplo de sistema de pagos anterior de PCT/EP2013/066540, puede ser de interés para la primera entidad restringir los pagos móviles en línea sin contacto mediante la aplicación del dispositivo móvil hasta que el usuario no haya finalizado con éxito el proceso de registro seguro (que comprende que el usuario seleccione un PIN para su uso en pagos móviles sin contacto).

En una implementación particular donde la primera entidad es un banco, el módulo servidor de pagos de PCT/EP2013/066540 podría incluso ser el mismo servidor que el referido en esta invención, asociado a las aplicaciones de software móvil protegidas. De modo que, en este caso, sería fácil restringir los pagos móviles en línea sin contacto hasta que la aplicación de software móvil protegida (denominada aplicación de teléfono móvil en PCT/EP2013/066540) haya sido registrada en los sistemas de la primera entidad mediante la inserción por el usuario de un código de activación en el dispositivo móvil y la selección de un PIN, requiriéndose el PIN para realizar pagos móviles sin contacto.

Ahora, la Fig. 2 de la presente invención combina el sistema descrito en la Fig. 1 de la presente invención con el sistema descrito en la Fig. 2b de PCT/EP2013/066540. Para facilitar la comprensión, los procesos ilustrados en la figura 2.b como etapas (5) a (14) se denominarán en este documento como etapa (7) en el contexto de la figura 2. Es decir, la etapa (7) de esta realización de la invención se refiere al proceso de registrar la aplicación de software móvil, seleccionando un PIN para pagos móviles en línea sin contacto, y obtener las credenciales para pagos móviles sin contacto.

De modo que en esta realización, la aplicación de software móvil protegida es utilizada para proporcionar un conjunto de servicios en línea al usuario y al menos uno de esos servicios en línea no está disponible para la aplicación de software móvil protegida hasta que se ha registrado en los sistemas de la primera entidad mediante la inserción por parte del usuario de un código de activación en el dispositivo móvil y la selección de un PIN, requiriéndose el PIN para tener acceso al al menos un servicio en línea.

También, como otra implementación particular donde la primera entidad es un banco y el módulo servidor de pagos de PCT/EP2013/066540 es el mismo servidor que el de la primera entidad al que se hace referencia en esta invención, los pagos móviles en línea sin contacto están restringidos hasta que la aplicación de software móvil protegida ha sido registrada en los sistemas de la primera entidad mediante la inserción por parte del usuario de un código de activación en el dispositivo móvil y la selección de un PIN, requiriéndose el PIN para realizar pagos móviles sin contacto, y hasta que la primera entidad descarga en la aplicación de software móvil protegida un conjunto de credenciales para su uso en los servicios de pagos móviles en línea sin contacto.

Para que se comprenda más fácilmente, los procesos ilustrados en la figura 2.b como etapas (5) a (14) se nombran como etapa (7) en el contexto de la figura 2. Es decir, la etapa (7) de esta realización de la invención se refiere al proceso de registrar la aplicación de software móvil y obtener las credenciales para pagos móviles sin contacto.

De modo que en esta realización, la aplicación de software móvil protegida se utiliza para proporcionar servicios de pagos móviles en línea sin contacto al usuario y esos servicios de pagos no están disponibles para la aplicación de software móvil protegida hasta que la primera entidad descarga a la aplicación de software móvil protegida al menos una parte de al menos una credencial para su uso en los servicios de pagos móviles en línea sin contacto.

Las Figuras 3a-3c ilustran una parte de otra realización de acuerdo con la invención. En esta parte de una realización, sólo se utiliza parte del registro de personalización de salida para generar la aplicación de software móvil protegida y otra parte se utiliza para futuras re-personalizaciones de seguridad de la aplicación de software móvil protegida.

De modo que utilizando esta realización los parámetros de seguridad y/o reglas de

ofuscación pueden ser renovadas en la aplicación de software móvil protegida cuando la personalización de seguridad actual expire o esté cerca de expirar.

En el contexto de esta realización, la figura 3.a muestra un archivo de personalización de salida con N registros de salida, cada uno con un identificador único.

El registro de personalización de salida 1 contiene un primer conjunto de parámetros de seguridad [ps_{11a}, ps_{11b}, ps_{11c},... ps_{11n}] asociados a un primer conjunto de reglas de ofuscación [ro_{11a}, ro_{11b}, ro_{11c},... ro_{11n}], un segundo conjunto de parámetros de seguridad [ps_{12a}, ps_{12b}, ps_{12c},... ps_{12m}] asociado a un segundo conjunto de reglas de ofuscación [ro_{12a}, ro_{12b}, ro_{12c},... ro_{12m}] ... y un n-ésimo conjunto de parámetros de seguridad [ps_{1na}, ps_{1nb}, ps_{1nc},... ps_{1nl}] asociado a un n-ésimo conjunto de reglas de ofuscación [ro_{1na}, ro_{1nb}, ro_{1nc},... ro_{1nl}] y

[ps_{11a}, ps_{11b}, ps_{11c},... ps_{11n}] y [ro_{11a}, ro_{11b}, ro_{11c},... ro_{11n}] se utilizan para personalizar inicialmente, en términos de parámetros de seguridad y reglas de ofuscación, la aplicación de software móvil protegida;

[ps_{12a}, ps_{12b}, ps_{12c},... ps_{12m}] y [ro_{12a}, ro_{12b}, ro_{12c},... ro_{12m}] se utilizarán para efectuar una primera re-personalización de la aplicación de software móvil protegida, en términos de parámetros de seguridad y reglas de ofuscación;

... ...

[ps_{1na}, ps_{1nb}, ps_{1nc},... ps_{1nl}] y [ro_{1na}, ro_{1nb}, ro_{1nc},... ro_{1nl}] se utilizarán para efectuar una (n-1) re-personalización de la aplicación de software móvil protegida, en términos de parámetros de seguridad y reglas de ofuscación;

y [$ps_{1(i-1)a}$, $ps_{1(i-1)b}$, $ps_{1(i-1)c}$,... $ps_{1(i-1)k}$] and [$ro_{1(i-1)a}$, $ro_{1(i-1)b}$, $ro_{(1(i-1)c}$,... $ro_{1(i-1)k}$] son sustituidos por [ps_{1ia}, ps_{1ib}, ps_{1ic},... ps_{1ij}] y [ro_{1ia}, ro_{1ib}, ro_{1ic},... ro_{1ij}] en el contexto del (i-1) proceso de re-personalización de seguridad. La misma lógica puede aplicarse a los registros de personalización de salida 2 a N.

En esta implementación particular se ha personalizado un conjunto de registros "vacíos" en la aplicación de software móvil protegida en la primera personalización de seguridad, de modo que al menos parte de ellos puedan utilizarse en el contexto de futuros procesos de re-personalización de seguridad.

En esta realización, algunos de los parámetros de seguridad personalizados en la aplicación de software móvil protegida son enviados a la primera entidad en el contexto de una conexión en línea desde la aplicación de software móvil protegida, y la primera entidad valida los parámetros de seguridad. En un ejemplo particular se envían [ps_{11a}, ps_{11b}, ps_{11c}] desde la aplicación de software móvil protegida a la primera entidad durante el proceso de registro de la aplicación, después de que la aplicación ha obtenido esos valores aplicando [ro_{11a}, ro_{11b}, ro_{11c}]. Si los valores no son correctos, la primera entidad no permitirá que se complete el proceso de registro, y deshabilitará la aplicación de software móvil protegida en sus sistemas. El resto de los parámetros de seguridad se enviará durante el ciclo de vida de la aplicación, para su validación por la primera entidad; si no son correctos, la aplicación será deshabilitada en los sistemas de la primera entidad.

La Figura 3.b muestra cómo ps_{11a} ha sido dividido en 4 partes y ofuscado en diferentes ubicaciones de la aplicación de software móvil protegida. La regla de ofuscación ro_{11a} se ha dividido en dos partes: una primera parte $ro_{11a(inicio)}$, que permite direccionar $ps_{11a(parte1)}$ desde el código de la aplicación, y una segunda parte $ro_{11a(parte1)}$ que permite direccionar desde el código de la aplicación la siguiente parte de ps_{11a}. Cada parte se refiere a la siguiente hasta aquella que ha sido etiquetada como la última parte en la regla de ofuscación. La Figura 3.b también muestra las ubicaciones vacías donde se pueden colocar futuros parámetros de seguridad y reglas de ofuscación. La Figura 3.c muestra el resultado de un proceso de re-personalización de seguridad donde ps_{12a}, asociado a la primera re-personalización del registro de salida 1, está ahora dividido en 5 partes y ofuscado en diferentes ubicaciones en la aplicación de software móvil protegida. De nuevo, La regla de ofuscación ro_{12a} se ha dividido en dos partes: una primera parte $ro_{12a(inicio)}$, que permite direccionar $ps_{12a(parte1)}$ desde el código de la aplicación, y una segunda parte $ro_{12a(parte1)}$ que permite direccionar desde el código de la aplicación la siguiente parte de ps_{12a}. La misma lógica puede aplicarse a cada uno de los parámetros / reglas de ofuscación y a cada uno de los registros de salida.

La Figura 3 es un ejemplo ilustrativo acerca del uso de parámetros de seguridad y reglas de ofuscación para proteger la aplicación de software móvil, y son posibles muchas variantes sin salirse de los principios de la presente invención. Como ejemplo particular, en función del valor de un parámetro incluido en el código de la aplicación de software móvil protegida, el código podría usar $ro_{11a(inicio)}$ para direccionar $ps_{11a(parte1)}$ cuando la personalización de seguridad es la inicial, y cambiando el valor de dicho parámetro, en la primera re-

personalización de seguridad, el código podría posteriormente usar $ro_{12a(inicio)}$ para direccionar $ps_{12a(parte1)}$ cuando la personalización de seguridad es la de la primera re-personalización. Las reglas de ofuscación pueden ser diferentes de las mostradas en estos ejemplos, según defina el primer emisor. Y también algunos de los parámetros de seguridad de la personalización inicial de seguridad podrían utilizarse, junto con partes del código de la aplicación, para crear una red de checksums del código durante la generación de la aplicación de software móvil protegida, siendo tales checksums embebidos y ofuscados en el código en el momento de la generación de la aplicación de software móvil protegida, y siendo los checksums del código diferentes de aquellos de otra aplicación de software móvil protegida calculados sobre los parámetros de seguridad diferentes de la primera personalización de seguridad de la otra aplicación de software móvil protegida.

Ventajosamente, debe remarcarse que antes de realizar una re-personalización los datos relacionados son completamente desconocidos por la aplicación de software móvil protegida, ya que esas reglas de ofuscación, y los parámetros de seguridad relacionados, están en ese momento sólo disponibles en los sistemas del proveedor de servicios (y en algunas ocasiones en los sistemas seguros de la segunda entidad).

De modo que en esta realización, al menos un dato del registro de personalización de salida no fue utilizado para generar la aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, y al menos parte de esos datos son enviados a la primera entidad, y la primera entidad re-personaliza al menos parcialmente la aplicación de software móvil protegida, en términos de al menos parte de los parámetros de seguridad y/o reglas de ofuscación, utilizando al menos parte de esos datos.

En un escenario diferente, se generan nuevos registros de personalización de salida por parte de la segunda entidad durante el ciclo de vida de las aplicaciones de software móvil protegidas y se envían a la primera entidad. Por tanto, utilizando esta realización los parámetros de seguridad y/o reglas de ofuscación pueden ser renovados por la primera entidad en la aplicación de software móvil protegida cuando todos los parámetros del registro de salida anterior hay sido usados o han expirado.

De modo que en otra realización, un nuevo registro de personalización de salida, asociado

al al menos un identificador único, es generado por la segunda entidad durante el ciclo de vida de una aplicación de software móvil protegida dada, y al menos parte de este nuevo registro de salida es enviado a la primera entidad, y la primera entidad re-personaliza al menos parcialmente la aplicación de software móvil protegida, en términos de al menos parte de los parámetros de seguridad y/o las reglas de ofuscación, utilizando datos incluidos en el nuevo registro de salida.

En una implementación particular de cualquiera de las dos realizaciones anteriores, se requiere que el usuario inserte su PIN en la aplicación de software móvil protegida, y la re-personalización de seguridad se efectúa cuando la primera entidad verifica que el usuario introdujo un valor de PIN correcto. De modo que cuando el usuario inserta el PIN para tener acceso a un servicio remoto del proveedor de servicios (por ejemplo, a través de un Servicio Web), la primera entidad puede aprovechar ese proceso en curso para re-personalizar la aplicación de software móvil protegida en términos de parámetros de seguridad y/o reglas de ofuscación.

En otra implementación particular, el proceso de re-personalización de seguridad es iniciado por la primera entidad en el contexto de una solicitud en línea a la primera entidad iniciada por la aplicación de software móvil protegida. En esta implementación, el proceso de re-personalización es iniciado por la primera entidad sin requerir que el usuario inserte el PIN, de modo que la primera entidad puede decidir realizar la re-personalización, por ejemplo, basándose en criterios de gestión del riesgo.

La Figura 1 también ilustra una parte de otra realización de acuerdo con la invención. En esta parte de una realización, hay un sistema de control de calidad a cargo de verificar si los parámetros de seguridad y/o reglas de ofuscación de los registros de salida han sido adecuadamente personalizados en las correspondientes aplicaciones de software móvil protegidas. Este sistema de control de calidad está diseñado para identificar cualquier error de personalización en la aplicación de software móvil protegida como resultado, por ejemplo, de un fallo eléctrico producido durante el proceso de personalización de seguridad. El objetivo es ser capaz de identificarlo antes de que la segunda entidad envíe una aplicación de software móvil protegida a la primera entidad.

La Figura 1 ilustra cómo una aplicación de software móvil protegida es generada en la etapa (4). De acuerdo con esta realización, la aplicación generada es enviada al sistema de control de calidad de la segunda entidad (figura 1.a) a cargo de determinar si hay algún error en la personalización de seguridad. En el contexto de este proceso, el sistema de control de calidad verificará también si los registros "vacíos" han sido adecuadamente personalizados en la aplicación de software móvil protegida. Si se ha producido un error de personalización, se reporta al sistema del software de ofuscación para que se repita el proceso de personalización de seguridad. Si la personalización ha sido correcta, la etapa (4) termina con el envío de la aplicación de software móvil protegida, y la asociación al correspondiente registro de salida e identificador único a las BBDD de la segunda entidad, según la invención.

De modo que en una realización, la aplicación de software móvil protegida es introducida en un sistema de control de calidad de la segunda entidad, a cargo de determinar si los parámetros de seguridad y/o las reglas de ofuscación han sido personalizados adecuadamente en la aplicación de software móvil protegida.

Aunque la presente invención se ha descrito con detalle a modo de ilustración, se entiende que tales detalles sólo tienen ese objetivo, y que para un experto en la materia será posible realizar variaciones en los mismos sin salirse del ámbito de la invención. Por tanto, aunque las realizaciones preferidas del método y del sistema móvil se han descrito con referencia el entorno en el que fueron desarrollados, son simplemente ilustrativos de los principios de la invención. Otras realizaciones y configuraciones se podrán diseñar si salirse del ámbito de las reivindicaciones adjuntas.

Además, aunque las realizaciones de la invención descritas con referencia a las figuras comprende aparatos de ordenador (en este documento, se entiende que un aparato de ordenador es cualquier medio electrónico de procesamiento capaz de ejecutar una secuencia de etapas codificadas como un programa) y procesos efectuados en aparatos de ordenador, la invención también se extiende a programas de ordenador, en particular programas de ordenador en o sobre una portadora, adaptados para llevar la invención a la práctica. El programa puede estar en forma de código fuente, código objeto, un código intermedio entre fuente y objeto como una forma parcialmente compilada, o cualquier otra forma adecuada para su uso en la implementación de los procesos de acuerdo con la

invención. La portadora puede ser cualquier entidad capaz de transportar el programa. Por ejemplo, la portadora puede comprender un medio de almacenamiento, como un ROM, por ejemplo un CD-ROM o un ROM de semiconductor, o un medio de almacenamiento magnético, por ejemplo un disco flexible o un disco duro. Además, la portadora puede ser una portadora transmisible como una señal eléctrica u óptica que puede transportarse a través de un cable eléctrico u óptico o por radio o de otro modo. Cuando el programa está incorporado en una señal que puede transmitirse directamente mediante un cable u otro dispositivo o medio, la portadora puede estar constituida por tal cable u otro dispositivo o medio. Alternativamente, la portadora puede ser un circuito integrado en el que está embebido el programa, estando adaptado el circuito integrado para llevar a cabo, o para su uso para llevar a cabo, los procesos relevantes.

REIVINDICACIONES

1. Un método para generar automáticamente aplicaciones de software de dispositivos móviles, donde cada una está personalizada de manera diferente en términos de parámetros de seguridad y/o reglas de ofuscación, comprendiendo dicho método las siguientes etapas:

a) una primera entidad, que es un proveedor de servicios, genera un conjunto de registros de entrada, conteniendo cada registro de entrada al menos un identificador único;

b) una segunda entidad, que es un personalizador de seguridad de aplicaciones de software de dispositivos móviles, recibe el conjunto de registros de entrada y utiliza el al menos un identificador único incluido en un registro de entrada para generar un registro de personalización de salida, donde este registro de salida es diferente de otro registro de salida generado a partir de otro registro de entrada en términos de parámetros de seguridad y/o reglas de ofuscación para la personalización;

c) la segunda entidad utiliza al menos parte de los datos del registro de salida, una réplica genérica de la aplicación de software de dispositivos móviles y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, siendo esta aplicación de software móvil protegida diferente en términos de parámetros de seguridad y/o reglas de ofuscación de otra aplicación obtenida utilizando al menos parte de otro registro de salida;

d) la segunda entidad envía las aplicaciones de software móvil protegidas a la primera entidad, cada una de ellas asociada a uno o varios identificadores únicos del correspondiente registro de entrada, y la primera entidad las almacena y también almacena la asociación a al menos uno de los identificadores únicos; y

e) un usuario solicita una réplica de la aplicación de software móvil a la primera entidad y una aplicación de software móvil protegida es descargada a un dispositivo móvil del usuario.

2. Un método de acuerdo con la reivindicación 1, donde la aplicación de software móvil protegida es introducida en un sistema de control de calidad de la segunda entidad, a cargo de determinar si los parámetros de seguridad y/o las reglas de ofuscación han sido adecuadamente personalizados en la aplicación de software móvil protegida.

3. Un método de acuerdo con la reivindicación 1 o 2, donde la segunda entidad almacena los registros de salida en al menos un archivo de salida y almacena el al menos un archivo de salida en sus sistemas.

4. Un método de acuerdo con la reivindicación 3, donde el al menos un archivo de salida es enviado por la segunda entidad a la primera entidad, y la primera entidad lo almacena en sus sistemas.

5. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 4, donde algunos de los parámetros de seguridad personalizados en la aplicación de software móvil protegida son enviados a la primera entidad en el contexto de una conexión en línea desde la aplicación de software móvil protegida, y la primera entidad valida los parámetros de seguridad.

6. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 5, donde la aplicación de software móvil protegida es descargada en el dispositivo móvil del usuario como resultado de otra aplicación, que ha sido instalada previamente en dicho dispositivo móvil del usuario, que se dirige a una dirección remota particular, y al menos uno de los servicios en línea no está disponible para la aplicación de software móvil protegida si un proceso de registro con éxito que requiere que el usuario introduzca un código de activación en la aplicación de software móvil protegida no ha sido completado dentro de un período de tiempo dado después de que la aplicación de software móvil protegida haya sido descargada en el dispositivo móvil del usuario, estando definido dicho período de tiempo por la primera entidad.

7. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 6, donde la aplicación de software móvil protegida se utiliza para proporcionar un conjunto de servicios en línea al usuario y al menos uno de esos servicios en línea no está disponible para la aplicación de software móvil protegida hasta que se ha registrado en los sistemas de la primera entidad mediante la introducción por parte del usuario de un código de activación en el dispositivo móvil y la selección de un PIN, requiriéndose el PIN para tener acceso al al menos un servicio en línea.

8. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 7, donde la aplicación de software móvil protegida es utilizada para proporcionar servicios de pagos móviles en línea sin contacto al usuario y dichos servicios de pagos no están disponibles para la aplicación de software móvil protegida hasta que la primera entidad descarga a la aplicación de software móvil protegida al menos una parte de al menos una credencial para su uso en los servicios de pagos móviles en línea sin contacto.

9. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 8, donde al menos un dato del registro de personalización de salida no fue utilizado para generar la aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, y al menos parte de esos datos son enviados a la primera entidad, y la primera entidad al menos parcialmente re-personaliza la aplicación de software móvil protegida, en términos de al menos parte de los parámetros de seguridad y/o reglas de ofuscación, utilizando al menos parte de esos datos.

10. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 9, donde un nuevo registro de personalización de salida, asociado al al menos un identificador único, es generado por la segunda entidad durante el ciclo de vida de una aplicación de software móvil protegida dada, y al menos parte de este nuevo registro de salida es enviado a la primera entidad, y la primera entidad re-personaliza al menos parcialmente la aplicación de software móvil protegida, en términos de al menos parte de los parámetros de seguridad y/o reglas de ofuscación, utilizando datos incluidos en el nuevo registro de salida.

11. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 10, donde uno o varios procesos pertenecientes al dominio de la primera entidad son proporcionados por la segunda entidad, o por un tercero de confianza, en nombre de la primera entidad.

12. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 11, donde uno o varios procesos de la segunda entidad son proporcionados por la primera entidad, o por un tercero de confianza, en nombre de la primera entidad.

13. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 12, donde la primera entidad asigna el al menos un identificador único del registro de entrada a un usuario particular antes de enviar el conjunto de registros de entrada a la segunda entidad, de modo que la aplicación de software móvil protegida ya está asignada a un usuario dado cuando es recibida por la primera entidad desde la segunda entidad.

14. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 12, donde la primera entidad asigna el al menos un identificador único del registro de entrada, y la aplicación de software móvil protegida, a un usuario particular después de haber recibido la correspondiente aplicación de software móvil protegida de la segunda entidad y después de que el usuario se haya registrado con éxito en un servicio del proveedor de servicios utilizando la aplicación de software móvil protegida.

15. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 12, donde la primera entidad asigna el al menos un identificador único del registro de entrada, y la aplicación de software móvil protegida, a un dispositivo móvil particular de un usuario después de haber recibido la correspondiente aplicación de software móvil protegida de la segunda entidad y después de que el usuario se haya registrado con éxito en un servicio del proveedor de servicios utilizando la aplicación de software móvil protegida.

16. Programa de ordenador que comprende instrucciones para hacer que un ordenador lleve a cabo el método de cualquiera de las reivindicaciones 1-15.

17. Programa de ordenador de acuerdo con la reivindicación 16, almacenado en un medio de almacenamiento.

18. Programa de ordenador de acuerdo con la reivindicación 16, soportado en una señal portadora.

19. Un sistema para generar automáticamente aplicaciones de software para dispositivos móviles, donde cada una está personalizada de manera diferente en términos de parámetros de seguridad y/o reglas de ofuscación, estando caracterizado dicho sistema por que comprende:

- una primera entidad que comprende:
    - medios electrónicos de procesamiento configurados para generar un conjunto de registros de entrada, conteniendo cada registro de entrada al menos un identificador único;
    - medios de almacenamiento configurados para almacenar aplicaciones de software móvil protegidas y una asociación de las mismas con al menos uno de los identificadores únicos;
    - medios de interfaz de usuario configurados para que un usuario solicite una réplica de la aplicación de software móvil; y
    - medios de transmisión configurados para descargar una aplicación de software móvil protegida a un dispositivo móvil del usuario, y
- una segunda entidad que comprende:
    - medios electrónicos de procesamiento configurados para personalizar las aplicaciones de software para dispositivos móviles, después de recibir el conjunto de registros de entrada, utilizando el al menos un identificador único

incluido en un registro de entrada para generar un registro de personalización de salida, donde el registro de salida es diferente de otro registro de salida, generado a partir de otro registro de entrada, en términos de parámetros de seguridad y/o reglas de ofuscación para la personalización; y

- medios de transmisión configurados para enviar las aplicaciones de software móvil protegidas a la primera entidad, estando cada una asociada a uno o varios identificadores únicos del correspondiente registro de entrada,

donde los medios de personalización de la segunda entidad introducen al menos parcialmente los datos del registro de salida en una réplica genérica de una aplicación de software para dispositivos móviles, y la segunda entidad utiliza la al menos parte del registro de salida, la réplica genérica de la aplicación de software para dispositivos móviles y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, siendo esta aplicación de software móvil protegida diferente en términos de parámetros de seguridad y/o reglas de ofuscación que otra obtenida utilizando al menos parte de otro registro de salida.

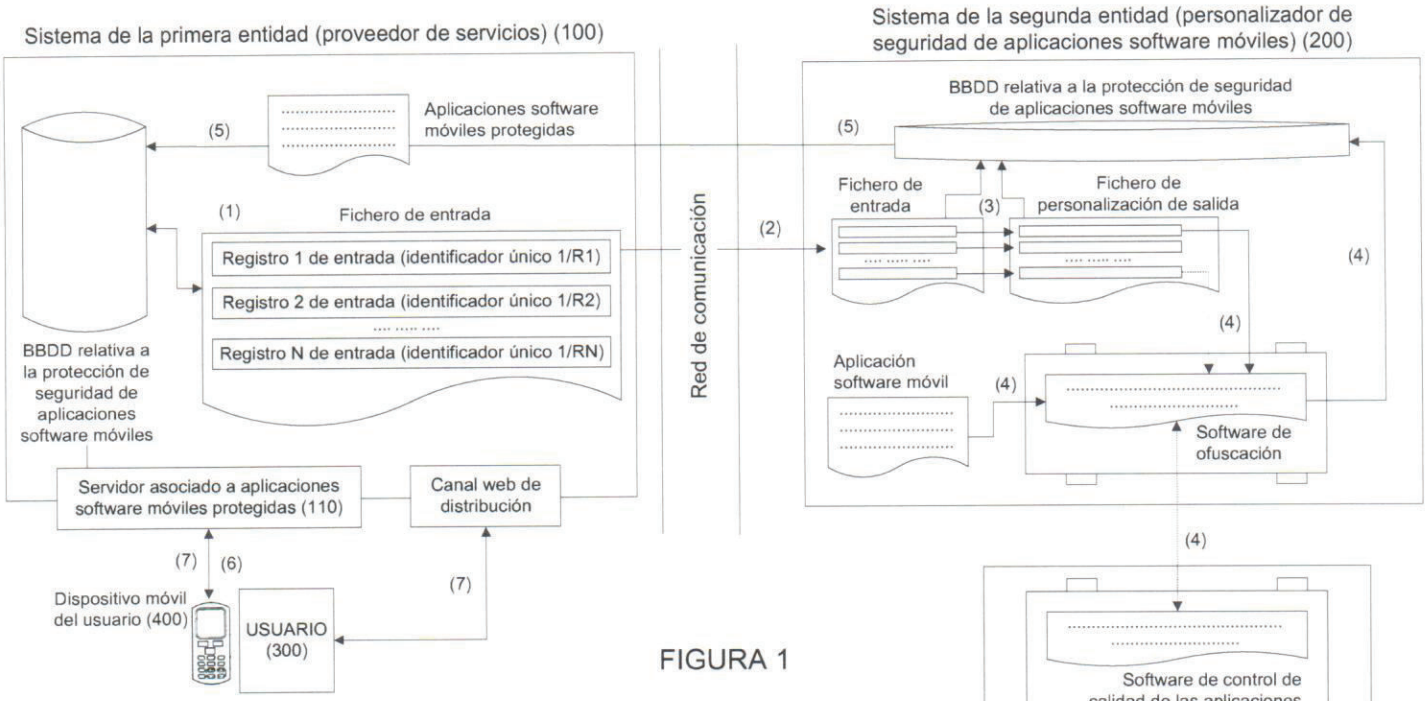
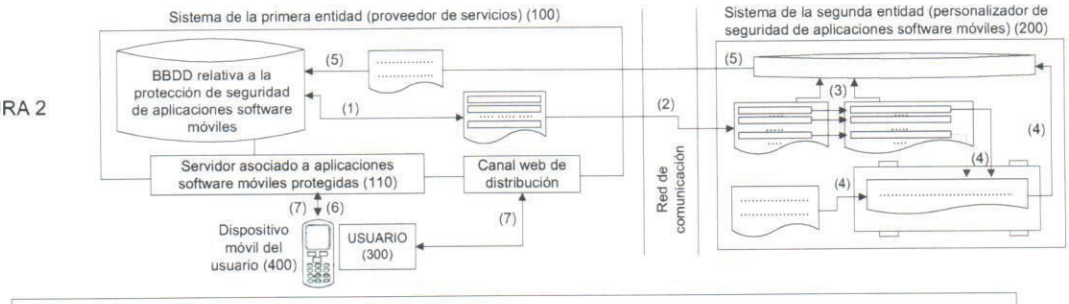


FIGURA 1

FIGURA 1.a

FIGURA 2



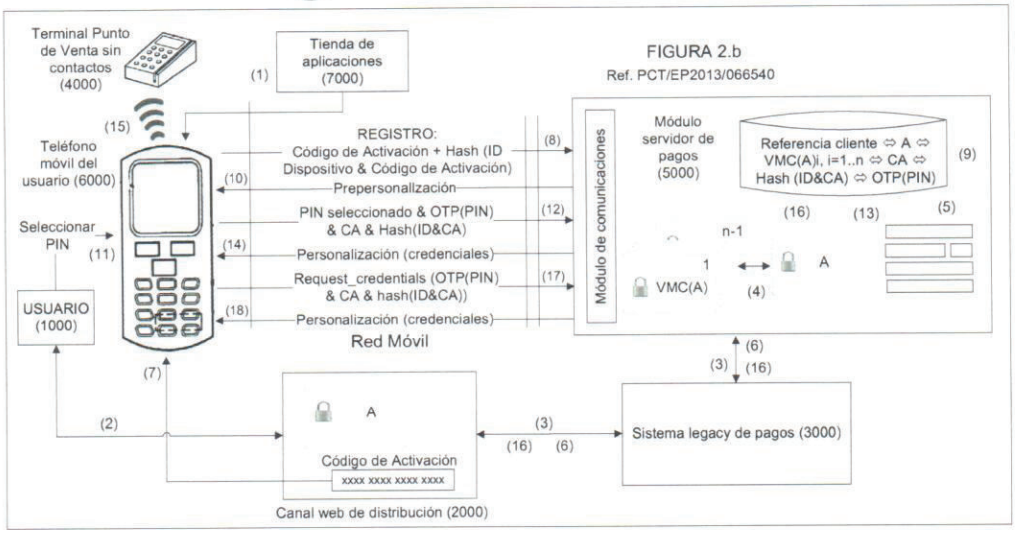


FIGURA 2.b
Ref. PCT/EP2013/066540

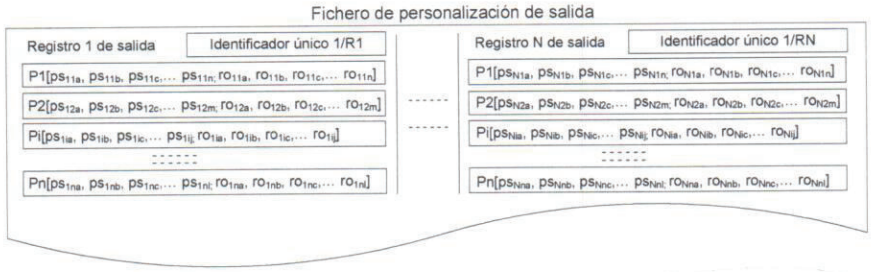


FIGURA 3.a

FIGURA 3

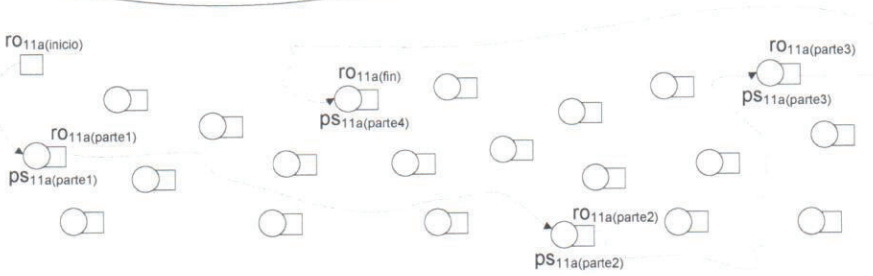


FIGURA 3.b

FIGURA 3.c

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201400211

(22) Fecha de presentación de la solicitud: 17.03.2014

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06F21/14*** (2013.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2005069138 A1 (DE JONG EDUARD K) 31.03.2005, párrafos [12],[65-77],[82-89],[96-98],[101-112],[115-123],[130]; figuras 1-17; reivindicaciones 12,19,45.	1,3-5,8-12,15-19
Y		2,6-7,13-14
Y	KR 20110072111 A (KOREA COPYRIGHT COMMISSION) 29.06.2011, resumen; figura 4.	2
Y	US 2011295708 A1 (SHIN JANGWOO) 01.12.2011, párrafos [7-8],[18],[33-51],[69-72]; figuras 1-3,7-8.	6-7,13-14
A	US 2009235089 A1 (CIET MATHIEU et al.) 17.09.2009, párrafos [3-4],[8-9],[12-20],[25-26]; figuras 1-2.	1
A	US 7054443 B1 (JAKUBOWSKI MARIUSZ H et al.) 30.05.2006, columna 2, líneas 41-47,56-62; columna 3, línea 56 – columna 4, línea 21; columna 5, líneas 15-25; columna 6, líneas 11-28; columna 7, líneas 23-45; columna 8, líneas 9-18,35-38; columna 9, líneas 39-45; columna 9, línea 59 – columna 10, líneas 9,34-42; figuras 1-2.	1-2,5,19
A	US 2009327091 A1 (HARTIN AMANDA ANNE et al.) 31.12.2009, párrafos [1],[3],[6-7],[18-21],[26-28]; figuras 1-3.	6-8

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
26.06.2015	J. M. Vázquez Burgos	1/7

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F, H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, INTERNET

Fecha de Realización de la Opinión Escrita: 26.06.2015

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-19	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-19	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2005069138 A1 (DE JONG EDUARD K)	31.03.2005
D02	KR 20110072111 A (KOREA COPYRIGHT COMMISSION)	29.06.2011
D03	US 2011295708 A1 (SHIN JANGWOO)	01.12.2011
D04	US 2009235089 A1 (CIET MATHIEU et al.)	17.09.2009
D05	US 7054443 B1 (JAKUBOWSKI MARIUSZ H et al.)	30.05.2006

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

La invención reivindicada divulga un método y un sistema para proteger aplicaciones de dispositivos móviles mediante ofuscación personalizada. El sistema se compone de una primera y una segunda entidad, y el método consiste en que la segunda genera una aplicación protegida a partir de la original mediante un software de ofuscación particularizado con unos registros obtenidos por la primera entidad, que contienen un identificador único. Cuanto un dispositivo solicita una aplicación protegida, se le asocia una de las versiones ofuscadas, que le es descargada.

El documento del estado de la técnica más próximo a la invención es D01 y divulga un método y un aparato para la ofuscación de programas, de forma que esta se personaliza en función de un identificativo del usuario.

Reivindicación 1

Seguidamente se reproduce en texto de la reivindicación 1 eliminando de él las referencias numéricas originales e insertando las del documento D01. Aquellas partes del texto que no figuran en D01 se señalan entre corchetes y en negrita.

Un método para generar automáticamente aplicaciones de software (párrafos 80-81) de dispositivos móviles (párrafo 89; 330), donde cada una está personalizada de manera diferente en términos de parámetros de seguridad y/o reglas de ofuscación (figura 3; párrafo 85), comprendiendo dicho método las siguientes etapas:

a) una [**primera**] entidad (415), que es un proveedor de servicios, genera un conjunto de registros de entrada, conteniendo cada registro de entrada al menos un identificador único (365; párrafos 82, 85);
b) [**una segunda entidad, que es un personalizador de seguridad de aplicaciones de software de dispositivos móviles**], recibe el conjunto de registros de entrada (1705) y utiliza el al menos un identificador único incluido en un registro de entrada para generar un registro de personalización de salida, donde este registro de salida es diferente de otro registro de salida generado a partir de otro registro de entrada en términos de parámetros de seguridad y/o reglas de ofuscación para la personalización (1725; figura 17A; párrafos 85, 123);
c) la [**segunda**] entidad utiliza al menos parte de los datos del registro de salida, una réplica genérica de la aplicación de software de dispositivos móviles y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, siendo esta aplicación de software móvil protegida diferente en términos de parámetros de seguridad y/o reglas de ofuscación de otra aplicación obtenida utilizando al menos parte de otro registro de salida (párrafos 85, 117-118);
d) la [**segunda**] entidad envía las aplicaciones de software móvil protegidas [**a la primera entidad**], cada una de ellas asociada a uno o varios identificadores únicos del correspondiente registro de entrada, y [**la primera entidad**] las almacena y también almacena la asociación (385) a al menos uno de los identificadores únicos (párrafos 84, 87); y
e) un usuario solicita una réplica de la aplicación de software móvil a la primera entidad (375) y
f) una aplicación de software móvil protegida es descargada a un dispositivo móvil del usuario (380).

La principal diferencia entre la invención reivindicada en 1 y el documento D01 del estado de la técnica más próximo es que en la primera se distinguen dos entidades, mientras que en la segunda no, de forma que sería una sola la que estaría a cargo de todos los pasos del procedimiento. Esta diferencia se concreta en que, los pasos b) y c) se situarían en el ofuscador (360), y el d) en la base datos (350), los a), e) y f) se ubicarían en la unidad (315) de D01, sin concretar más. El efecto técnico de esta diferencia sería el de no asignar unos medios de almacenamiento y procesamiento concretos, asociados a la base de datos (350), que permitiesen delimitar una entidad separada, para las funciones relativas a la recepción y posterior procesamiento de las solicitudes recibidas de los terminales móviles, así como para el envío a estos del resultado del ofuscador, almacenado en la base de datos. El problema técnico objetivo por tanto sería el de situar estas funciones en unos medios de almacenamiento y procesamiento ad hoc. Teniendo en cuenta que la arquitectura utilizada en D01 para la implementación de su solución (párrafo 82; figura 2) contempla el uso modular de memorias y medios de procesamiento y la disponibilidad de interfaces WAN y LAN, así como que gran parte de las funciones se han segregado en bloques funcionalmente diferentes (figura 3), semejante problema podría ser resuelto por un experto en la materia sin necesidad del recurso a la actividad inventiva.

A los ejemplos contenidos en el documento D01 de técnicas de ofuscación personalizables, el documento D04 añade otro basado en el uso de un juego de funciones de ofuscación.

En consecuencia, se concluye que, a la luz de D01, la invención reivindicada en 1 no reúne el requisito de actividad inventiva, conforme se establece este requisito en el artículo 8 de la Ley de Patentes de 1986.

Reivindicaciones 2 a 18

Con respecto al objeto de la reivindicación 2, y en concreto a la verificación de la personalización de la ofuscación, el documento D01 contendría un procedimiento para ello, que no es otro que el empleado en el dispositivo de usuario para ejecutar la aplicación protegida; caso de que esta hubiera sido por ejemplo defectuosamente personalizada, no sería posible ejecutar la aplicación. No así ocurre con la ubicación de dicho procedimiento en otra unidad que no sea dicho dispositivo de usuario, como una de control. A este respecto, el documento D02 muestra un sistema de ofuscación de software con una unidad de verificación de dicha ofuscación. Un experto en la materia combinaría el documento D01 del estado más próximo de la materia con las partes relevantes de D02, con el fin de obtener las características reivindicadas en 2 con una expectativa razonable de éxito.

El almacenamiento de los registros de salida en un archivo reivindicado en 3 estaría incluido en D01 (párrafos 82, 115, 130; reivindicación 45), lo mismo que el almacenamiento reivindicado en 4 (párrafo 87; reivindicación 45).

La conexión en línea de las unidades, reivindicada en 5, aunque no explícitamente incluida en D01, sí lo estaría implícitamente (párrafo 82) al poder contar estas con interfaces de LAN o WAN. En cualquier caso, su implementación es una técnica muy conocida para un experto en materia, que no requeriría para ello de actividad inventiva por su parte. El documento D05 muestra un ejemplo de una arquitectura distribuida de este tipo, orientada a la provisión de aplicaciones protegidas en terminales móviles. A su vez, la verificación de los parámetros de seguridad estaría incluida en D01, por cuanto este documento contempla el caso en que la ofuscación se define conforme una tabla de códigos de instrucciones, de un conjunto de tablas generado a partir de un proceso aleatorio, de forma que es la unidad proveedora de software la que decide cuál se selecciona para la ofuscación (párrafo 117; figura 15), en lo que constituiría una validación, en el sentido en que se hace dicha tabla válida para la ofuscación, y una personalización en cuanto a que una tabla única se asigna a un dispositivo concreto.

Con respecto al objeto de 6, el documento D03 muestra un sistema de activación de aplicaciones protegidas en terminales móviles, donde (párrafos 37, 39) la misma exige de la introducción de una clave de activación válida por un tiempo, dotada de una marca de tiempo al objeto de verificar su expiración temporal, antes del que el usuario debería de introducirla.

La exigencia de registro previo reivindicada en 7 estaría también incluida en D03 (párrafos 18, 40, 42, 44, 51).

Con respecto a la exigencia de credenciales contenida en 8, cabe considerar que se incluye en D01, ya que la información secreta que se transmite al dispositivo de usuario constituye una credencial, puesto que está ligada tanto al ID del dispositivo como al proveedor del software (figura 3; párrafo 105). Asimismo, también lo estaría en D03, puesto que en este documento, las claves proporcionadas contienen una licencia del publicador o vendedor del software (párrafos 33-34; figura 3).

Un experto en la materia combinaría el documento D01 del estado más próximo de la materia con las partes relevantes de D03, con el fin de obtener las características reivindicadas en 6 o 7 u 8 con una expectativa razonable de éxito.

Con relación al objeto de 9, en D01 se contempla un caso que lo incluiría (párrafo 130), donde se abre el procedimiento a la posibilidad de utilizar un mayor o menor número de tablas de asignación de instrucciones (números que serían homologables a los registros de entrada al programa de ofuscación) en función de la cantidad de memoria disponible en el tiempo, variándose si lo hace dicha cantidad de memoria. Esto es, el número de registros se liga al consumo de memoria y se usan más o menos según este sea asumible o no. También estaría incluido el de la reivindicación 10 (párrafo 123), puesto que se considera la posibilidad de generar correspondencias de instrucciones (1765) adicionales, a partir de una clave ligada al mismo identificador único, que puedan ser utilizadas posteriormente.

Las posibilidades objeto de 11 y 12 serían satisfechas por una fusión de las dos unidades, que estaría contemplada en D01 (figura 3).

Con respecto al objeto de 13, el documento D01 contempla un procedimiento donde los registros que sirven de entrada (1705) para la generación de aquellos que dirigen el proceso de ofuscamiento (1725) están ya asociados en origen a un identificativo de dispositivo de usuario (figura 17A; párrafos 123). Dicha asociación es con un dispositivo en D01, pero no con un usuario como tal. Algo que sí figura en D03 (párrafo 47).

El objeto de 14 puede considerarse también incluido en D01 con la misma salvedad respecto al uso de identificativo de dispositivo en lugar del de usuario. En concreto, el párrafo 117 y la figura 15 describen el caso de uso de registros de entrada generados aleatoriamente y pertenecientes a un conjunto cuyos componentes han sido previamente identificados en el proveedor de aplicaciones y el dispositivo de usuario, de manera que la aplicación protegida se envía conjuntamente con dicha identificación, de forma que es una vez generada dicha aplicación que se asigna a un usuario determinado.

Un experto en la materia combinaría el documento D01 del estado de la técnica más próximo con las características relevantes de D03 con el fin de obtener las de las invenciones reivindicadas en 13 o 14 con una expectativa razonable de éxito.

Dado que el objeto de 15 es similar al de 14 pero utilizando esta vez un identificativo de dispositivo, cabe concluir sobre él que está incluido en D01.

El contenido de las reivindicaciones 16 a 18 se correspondería con diferentes realizaciones software de la invención contempladas en D01 (párrafos 65, 82-83; reivindicaciones 12, 19).

En consecuencia, a la vista de las consideraciones anteriores, y una vez tenidas en cuenta las correspondientes relaciones de dependencia de cada una de las reivindicaciones 2 a 19, cabe concluir lo siguiente:

A la luz de D01, las invenciones reivindicadas en 3, 4, 5, 8, 9, 10, 11, 12, 15, 16, 17 y 18 no reunirían el requisito de actividad inventiva, tal y como este se define en el artículo 8 de la Ley de Patentes de 1986.

A la luz de la combinación de los documentos D01 y D02, la invención reivindicada en 2 no reuniría el requisito de actividad inventiva, tal y como este se define en el artículo 8 de la Ley de Patentes de 1986.

A la luz de la combinación de los documentos D01 y D03, las invenciones reivindicadas en 6, 7, 13 y 14 no reunirían el requisito de actividad inventiva, tal y como este se define en el artículo 8 de la Ley de Patentes de 1986.

Reivindicación 19

Seguidamente se reproduce en texto de la reivindicación 19 eliminando de él las referencias numéricas originales e insertando las del documento D01. Aquellas partes del texto que no figuran en D01 se señalan entre corchetes y en negrita.

Un sistema para generar automáticamente aplicaciones de software (párrafos 80-81) para dispositivos móviles (párrafo 89; 330), donde cada una está personalizada de manera diferente en términos de parámetros de seguridad y/o reglas de ofuscación (figura 3; párrafo 85), estando caracterizado dicho sistema por que comprende:

- una [**primera**] entidad que comprende:
  - medios electrónicos de procesamiento (párrafo 82) configurados para generar un conjunto de registros de entrada (1700, 1705; párrafo 121) , conteniendo cada registro de entrada al menos un identificador único;
  - medios de almacenamiento (párrafo 82) configurados para almacenar aplicaciones de software móvil protegidas (450) y una asociación de las mismas con al menos uno de los identificadores únicos (485);
  - medios de interfaz de usuario configurados para que un usuario solicite una réplica de la aplicación de software móvil (220); y
  - medios de transmisión (310) configurados para descargar una aplicación de software móvil protegida a un dispositivo móvil del usuario, y
- [**una segunda entidad que comprende:**]
  - medios electrónicos de procesamiento (párrafo 82) configurados para personalizar las aplicaciones de software para dispositivos móviles, después de recibir el conjunto de registros de entrada, utilizando el al menos un identificador único incluido en un registro de entrada para generar un registro de personalización de salida (1725), donde el registro de salida es diferente de otro registro de salida, generado a partir de otro registro de entrada, en términos de parámetros de seguridad y/o reglas de ofuscación para la personalización; y
  - medios de transmisión (310) configurados para enviar las aplicaciones de software móvil protegidas a la primera entidad, estando cada una asociada a uno o varios identificadores únicos del correspondiente registro de entrada,

donde los medios de personalización de la [**segunda**] entidad introducen al menos parcialmente los datos del registro de salida en una réplica genérica de una aplicación de software para dispositivos móviles, y la [**segunda**] entidad utiliza la al menos parte del registro de salida, la réplica genérica de la aplicación de software para dispositivos móviles y software de ofuscación para generar una aplicación de software móvil protegida que está asociada al registro de salida y al al menos un identificador único, siendo esta aplicación de software móvil protegida diferente en términos de parámetros de seguridad y/o reglas de ofuscación que otra obtenida utilizando al menos parte de otro registro de salida (párrafos 121-123; figuras 17).

La diferencia entre la invención reivindicada en 19 y el documento D01 del estado de la técnica más próximo sería que la primera reparte los medios de procesamiento y memoria entre dos unidades diferenciadas, mientras que el segundo no explicita semejante reparto. El efecto técnico que tiene esta diferencia es el de permitir una configuración, gestión y mantenimiento separado e independiente para cada uno de los dos grupos de memoria y medios de procesamiento, exigiendo al mismo tiempo una conexión entre ellos. El problema técnico objetivo a resolver sería por tanto distribuir las funciones descritas en D01 conforme el reparto establecido en 19, entre los dos conjuntos de memoria y medios de procesamiento según corresponda, dotándolos de los medios para comunicarse entre ellos. Teniendo en cuenta que la arquitectura utilizada en D01 para la implementación de su solución (párrafo 82; figura 2; reivindicación 45) contempla el uso modular de memorias y medios de procesamiento y la disponibilidad de interfaces WAN y LAN, así como que gran parte de las funciones se han segregado en bloques funcionalmente diferentes (figura 3), semejante problema podría ser resuelto por un experto en la materia sin necesidad del recurso a la actividad inventiva.

En consecuencia, se concluye que, a la luz de D01, la invención reivindicada en 19 no reúne el requisito de actividad inventiva, tal y como este se define en el artículo 8 de la Ley de Patentes de 1986.