(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 814 877**

(51) Int. CI.:

G06F 21/12 (2013.01)
G06F 21/14 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.07.2016 E 16178926 (8)**

(97) Fecha y número de publicación de la concesión europea: **10.06.2020 EP 3270310**

(54) Título: **Protección de seguridad de aplicaciones de dispositivos móviles basada en personalización y vinculación segura de dominios de código**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.03.2021

(73) Titular/es:

AFIRMA CONSULTING & TECHNOLOGIES, S.L. (100.0%)
C/ Julio Palacios, 13, 8°
28029 Madrid, ES

(72) Inventor/es:

PÉREZ LAFUENTE, CARLOS ALBERTO

(74) Agente/Representante:

LORENTE BERGES, Ana

DESCRIPCIÓN

Protección de seguridad de aplicaciones de dispositivos móviles basada en personalización y vinculación segura de dominios de código

Ámbito técnico

Esta invención es relativa a métodos y aparatos para personalizar automáticamente en términos de seguridad aplicaciones software de dispositivos móviles, estando la personalización asociada a vinculación segura de dominios de código.

Antecedentes

En las tecnologías móviles actuales numerosas aplicaciones móviles son protegidas usando elementos seguros tales como tarjetas SIM, chips embebidos o tarjetas micro-SD. A pesar de que esos contenedores seguros ofrecen una alta resistencia a la manipulación, aspectos de control de negocio hacen que los proveedores de servicios busquen alternativas para proteger los activos sensibles (tales como claves y datos secretos) de sus aplicaciones móviles, y las propias aplicaciones móviles.

Dentro de dichas alternativas la ofuscación de código y la criptografía white box, en combinación con otras técnicas, son usadas para proteger aplicaciones software de dispositivos móviles. Idealmente, cada aplicación debería ser protegida de una forma personalizada, pero a veces dicha personalización puede introducir complejidad adicional en términos de instalación y gestión de la aplicación.

El arte previo revela métodos para generar automáticamente aplicaciones software protegidas de dispositivos móviles mediante el uso de software de ofuscación, en donde una aplicación software protegida resultante dada de dispositivo móvil puede ser diferente que cualquier otra en términos de parámetros de seguridad y/o reglas de ofuscación. Dentro de dichos métodos el(los) fichero(s) binario(s) de aplicación resultantes de una protección de seguridad dada serían diferentes que el(los) fichero(s) binario(s) de aplicación resultantes de una protección de seguridad diferente de la misma versión de la aplicación.

Sin embargo, los mercados más populares de distribución de aplicaciones software de dispositivos móviles (ej. Google Play Store o Apple Store) no están actualmente habilitados para distribuir diferentes ficheros(s) binarios/ejecutables para diferentes grupos de usuarios, en relación a una versión dada de una aplicación. El(los) fichero(s) binario(s) son los mismos para todos los usuarios de dispositivos móviles que descargan e instalan una versión dada de la aplicación.

Considerando las limitaciones anteriores, la distribución de dicho(s) fichero(s) binario(s) para diferentes grupos de usuarios puede requerir el uso de servidores de distribución de aplicaciones diferentes que los de un mercado de aplicaciones (ej. servidores del proveedor de servicios propietario de la aplicación). Esto puede impactar en usabilidad, y a veces puede incluso no estar permitido por el propietario del sistema operativo del dispositivo móvil.

Para evitar los referidos problemas, dentro de esta invención el fichero(s) binario(s) asociado a una versión dada de una aplicación es el mismo para todos los usuarios de dispositivos móviles, pero se aplica una personalización de seguridad a la aplicación software protegida de dispositivo móvil de tal forma que dicha personalización está asociada a procesos seguros de vinculación de dominios de código, de forma que se consigue un aumento notable de la protección de la aplicación software de dispositivo móvil en los dispositivos móviles de los usuarios.

Por tanto, esta nueva invención revela métodos relativos a aplicaciones software protegidas de dispositivos móviles que incluyen varios dominios de código, relativos a uno o varios proveedores de servicios, donde al menos parte de ellos están en un estado no-personalizado de seguridad que les deshabilita para operación normal cuando la aplicación es distribuida e instalada en un dispositivo móvil de usuario, y uno o varios de esos dominios de código son personalizados posteriormente en la aplicación software protegida de dispositivo móvil mediante métodos y técnicas de personalización de seguridad que los habilitan para operación normal y que están basados en vincular en términos de seguridad uno o más de los dominios de código con otros uno o más de los dominios de código.

Ventajosamente, estos métodos y técnicas permiten mejorar la protección de la aplicación en términos de proteger activos sensibles y procesos críticos de la aplicación de una forma personalizada, como se describe a continuación.

Resumen de la invención

Lo que se revela aquí son nuevos métodos y aparatos para personalizar una aplicación software de dispositivo móvil en términos de seguridad, donde uno o más primeros dominios de código son vinculados en términos de seguridad a uno o más segundos dominios de código a través de una personalización de seguridad que es requerida para habilitar los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones esto se consigue proporcionando un método asociado con uno o más proveedores de servicios y un proveedor de servicios de personalización en relación a la personalización de seguridad de una aplicación software de dispositivo móvil en un dispositivo móvil de un usuario, el método incluyendo:

usando por el proveedor de servicios de personalización una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad que están almacenados en una o más memorias para generar usando uno o más dispositivos de procesamiento una aplicación software protegida de dispositivo móvil que es personalizada en términos de seguridad usando datos del registro de personalización de seguridad, la aplicación generada incluyendo varios dominios de código, relativos a los uno o más proveedores de servicio, donde uno o más primeros dominios de código son vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar los uno o más primeros dominios de código para operación regular;

enviando la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada desde el proveedor de servicios de personalización a un servidor de distribución, dicho estado deshabilitando los uno o más primeros dominios de código para operación regular, y la aplicación software protegida de dispositivo móvil siendo almacenada en una o más memorias del servidor de distribución;

recibiendo desde el dispositivo móvil del usuario una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada;

enviando datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario, a la aplicación software protegida de dispositivo móvil no personalizada en seguridad en el dispositivo móvil del usuario, los datos de personalización de seguridad habilitando en la aplicación al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones el proveedor de servicios de personalización es uno de los uno o más proveedores de servicios.

Conforme a algunas implementaciones el habilitado de el al menos uno de los uno o más primeros dominios de código está asociado a uno o más parámetros de seguridad relativos al registro de personalización de seguridad de ciclo de vida, que son diferentes que los correspondientes del registro de personalización de seguridad.

Conforme a algunas implementaciones la personalización de seguridad asociada al registro de personalización de seguridad de ciclo de vida es relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código son recibidas desde el dispositivo móvil del usuario, cada solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida son enviados a la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular. Ventajosamente diferentes grupos de uno o más primeros dominios de código no-habilitados son personalizados en términos de seguridad en diferentes instantes

temporales, por lo que un atacante necesitaría realizar diferentes ataques a cada aplicación software protegida de dispositivo móvil a lo largo de su ciclo de vida de personalización de seguridad para intentar gradualmente explotar la funcionalidad cubierta por cada uno o más primeros dominios de código que ya han sido habilitados para operación regular.

Conforme a algunas implementaciones al menos uno del otro uno o más primeros dominios de código está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados a una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a los uno o más primeros dominios de código.

Conforme a algunas implementaciones uno o más dispositivos de procesamiento hacen una aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad expirar si una solicitud para una personalización de seguridad de al menos otro uno o más primeros dominios de código es recibida más tarde que un periodo de tiempo predefinido después de que datos de personalización de seguridad relativos a una solicitud previa para una personalización de seguridad de al menos uno u otro diferente uno de los uno o más primeros dominios de código fue enviada a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada o parcialmente-personalizada. Limitando la ventana de tiempo permitida entre dos procesos diferentes de personalización parcial de seguridad de uno o más primeros dominios de código, activos sensibles gestionados por la aplicación entre una personalización de seguridad y otra posterior pueden ser mejor protegidos.

Conforme a algunas implementaciones los uno o más primeros/segundos dominios de código asociados en una o más memorias del proveedor de servicios de personalización a la aplicación software protegida de dispositivo móvil en un dispositivo móvil de un primer usuario son diferentes que los uno o más primeros/segundos dominios de código asociados en una o más memorias del proveedor de servicios de personalización a la aplicación software protegida de dispositivo móvil en un dispositivo móvil de un segundo usuario.

Conforme a algunas implementaciones datos de re personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida, o a otro registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario, son enviados a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad parcialmente-personalizada o personalizada, los datos de re personalización de seguridad son al menos parcialmente diferentes que los datos de personalización de seguridad y habilitan en la aplicación para operación regular al menos uno de los uno o más primeros dominios de código y/o al menos uno del otro uno o más primeros dominios de código.

Conforme a algunas implementaciones al menos uno del otro uno o más primeros dominios de código está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código a través de la re personalización de seguridad, dicha re personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en el uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados a una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a los uno o más primeros dominios de código.

Conforme a algunas implementaciones uno o más primeros dominios de código asociados a un primer proveedor de servicios pueden ser habilitados para operación regular por el proveedor de servicios de personalización independientemente de la habilitación para operación regular de otros uno o más primeros dominios de código asociados a un segundo proveedor de servicios.

Conforme a algunas implementaciones hay un método asociado con el uso de un dispositivo móvil de un usuario en relación a la personalización de seguridad de una aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario, la aplicación software protegida de dispositivo móvil previamente generada por un proveedor de servicios de personalización en un estado de seguridad personalizada usando una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad, la aplicación protegida incluyendo varios dominios de código, relativos a uno o más proveedores de servicios, donde uno o más primeros dominios de código quedan vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad asociada al registro de personalización de seguridad, el método incluyendo:

solicitando desde el dispositivo móvil del usuario una aplicación software de dispositivo móvil a un servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada;

recibiendo desde el servidor de distribución y a continuación instalando por uno o más dispositivos de procesamiento en el dispositivo móvil la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código están deshabilitados para operación regular;

enviando desde el dispositivo móvil del usuario una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estado en un estado de seguridad no-personalizada;

recibiendo datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no-personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones el habilitado de el al menos uno de los uno o más primeros dominios de código está asociado a uno o más parámetros de seguridad relativos al registro de personalización de seguridad de ciclo de vida, que son diferentes que los correspondientes del registro de personalización de seguridad.

Conforme a algunas implementaciones solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código son enviadas desde el dispositivo móvil del usuario al proveedor de servicios de personalización, cada solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario son recibidos en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

Conforme a algunas implementaciones al menos uno del otro uno o más primeros dominios de código está vinculado en términos de seguridad a uno o más primeros dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular están disponibles en una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a uno o más primeros dominios de código que han sido previamente habilitados para operación regular.

Conforme a algunas implementaciones una solicitud para una personalización de seguridad de al menos otro uno o más primeros dominios de código es enviada desde el dispositivo móvil del usuario al proveedor de

servicios de personalización posteriormente a de un periodo de tiempo predefinido después de que datos de personalización de seguridad relativos a una solicitud previa para una personalización de seguridad de al menos uno u otro diferente uno de los uno o más primeros dominios de código fueran recibidos en la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada o parcialmente-personalizada, y una notificación desde el proveedor de servicios de personalización indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado es recibida en el dispositivo móvil del usuario.

Conforme a algunas implementaciones el uno o más primeros dominios de código habilitados mediante primeros datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un primer usuario son diferentes que los uno o más primeros dominios de código habilitados mediante segundos datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un segundo usuario.

Conforme a algunas implementaciones los datos de personalización de seguridad recibidos en el dispositivo móvil de un primer usuario, los datos habilitando en la aplicación uno o más primeros dominios de código para operación regular y asociados a un primer registro de personalización de seguridad de ciclo de vida que incluye primeros parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código, son diferentes que los datos de personalización de seguridad recibidos en el dispositivo móvil de un segundo usuario, los datos habilitando en la aplicación uno o más primeros dominios de código para operación regular y asociados a un segundo registro de personalización de seguridad de ciclo de vida que incluye segundos parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código.

Conforme a algunas implementaciones datos de re personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida, o a otro registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario, son recibidos en la aplicación software protegida de dispositivo móvil estando en un estado de seguridad parcialmente-personalizada o personalizada, los datos de re personalización de seguridad son al menos parcialmente diferentes que los datos de personalización de seguridad y habilitan en la aplicación para operación regular al menos uno de los uno o más primeros dominios de código y/o al menos uno del otro uno o más primeros dominios de código.

Un medio leíble no transitorio de ordenador almacenando código leíble de programa de ordenador para causar un procesador de un dispositivo móvil de un usuario realizar un método asociado a la personalización de seguridad de una aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario, la aplicación software protegida de dispositivo móvil previamente generada por un proveedor de servicios de personalización en un estado de seguridad personalizada usando una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad, la aplicación protegida incluyendo varios dominios de código, relativos a uno o más proveedores de servicios, donde uno o más primeros dominios de código quedan vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad asociada al registro de personalización de seguridad, el método incluyendo:

solicitando desde el dispositivo móvil del usuario una aplicación software de dispositivo móvil a un servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada;

recibiendo desde el servidor de distribución y a continuación instalando por uno o más dispositivos de procesamiento en el dispositivo móvil la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código están deshabilitados para operación regular;

enviando desde el dispositivo móvil del usuario una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estado en un estado de seguridad no-personalizada;

recibiendo datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no-personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de

código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones un medio leíble no transitorio de ordenador almacenando código leíble de programa de ordenador es provisto que causa el procesador enviando solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código desde el dispositivo móvil del usuario al proveedor de servicios de personalización, cada solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y recibiendo datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

Conforme a algunas implementaciones un dispositivo móvil de un usuario es provisto que está asociado con la personalización de seguridad de una aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario, la aplicación software protegida de dispositivo móvil previamente generada por un proveedor de servicios de personalización en un estado de seguridad personalizada usando una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad, la aplicación protegida incluyendo varios dominios de código, relativos a uno o más proveedores de servicios, donde uno o más primeros dominios de código quedan vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad asociada al registro de personalización de seguridad, el dispositivo móvil incluyendo:

un medio de almacenamiento electrónico que almacena datos de personalización de seguridad; y

un procesador adaptado a:

solicitar una aplicación software de dispositivo móvil a un servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no personalizada;

recibir desde el servidor de distribución y a continuación instalar en el dispositivo móvil la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código estas deshabilitados para operación regular;

enviar una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no personalizada;

recibir datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no-personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones el procesador está adaptado para enviar solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código desde el dispositivo móvil del usuario al proveedor de servicios de personalización, cada solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y para recibir datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático ilustrando métodos y aparatos conforme a algunas implementaciones, relativas a uno o más proveedores de servicios y un proveedor de servicios de personalización en relación a la personalización de seguridad de una aplicación software de dispositivo móvil, en donde una descripción más detallada es provista en relación al proveedor de servicio 1 y al proveedor de servicios de personalización.

Las figuras 2.a a 2.l son diagramas esquemáticos ilustrando métodos y aparatos conforme a algunas implementaciones en relación a la personalización de seguridad de una aplicación software de dispositivo móvil. En particular:

- La figura 2.a ilustra registros de personalización de seguridad generados por el proveedor de servicios de personalización y es también relativa a la generación de una aplicación software protegida de dispositivo móvil personalizada en seguridad.
- La figura 2.b ilustra algunas implementaciones donde una aplicación software de dispositivo móvil ha sido desarrollada para realizar funciones asociadas a un proveedor de servicios que es la misma entidad que el proveedor de servicios de personalización.
- La figura 2.c ilustra algunas implementaciones de aplicar una protección de seguridad a funciones en primeros dominios de código, en el contexto de generar una aplicación software protegida de dispositivo móvil.
- La figura 2.d ilustra algunas implementaciones asociadas a la protección de al menos partes de parámetros de seguridad, reglas de ofuscación y redes de checksums en una parte de la base de datos de la aplicación que está asociada a un dominio de código dado, en el contexto de generar una aplicación software protegida de dispositivo móvil.
- La figura 2.e ilustra un conjunto de registros de personalización de seguridad con valores por defecto (/erróneos) que pueden ser usados para propósitos de test.
- La figura 2.f ilustra una personalización de seguridad que usa valores por defecto y escenarios de test.
- La figura 2.g ilustra algunas implementaciones asociadas a la protección de datos de personalización de seguridad asociados a la aplicación software protegida de dispositivo móvil instalada en el dispositivo móvil de un primer y de un segundo usuario.
- La figura 2.h ilustra algunas implementaciones donde el dispositivo móvil de un primer usuario almacena datos de personalización de seguridad que habilitan primeros dominios de código para operación regular.
- La figura 2.i ilustra algunas implementaciones donde el dispositivo móvil de un primer usuario almacena datos de personalización de seguridad que habilitan primeros dominios de código y otros primeros dominios de código para operación regular.
- La figura 2.j ilustra algunas implementaciones donde el dispositivo móvil de un segundo usuario almacena datos de personalización de seguridad que habilitan primeros dominios de código y otros primeros dominios de código para operación regular.
- La figura 2.k ilustra algunas implementaciones asociadas a la protección de datos de re personalización de seguridad asociados a la aplicación software protegida de dispositivo móvil instalada en el dispositivo móvil de un segundo usuario.
- La figura 2.l ilustra algunas implementaciones donde el dispositivo móvil de un segundo usuario almacena datos de re personalización de seguridad que habilitan primeros dominios de código y otros primeros dominios de código para operación regular.

La figura 3 es un diagrama esquemático ilustrando métodos y aparatos donde la aplicación software protegida de dispositivo móvil es relativa a varios proveedores de servicios y una arquitectura equivalente a la ilustrada en la figura 2.b es replicada en el código de aplicación para cada uno de los proveedores de servicios.

Descripción detallada

La figura 1 es un diagrama esquemático ilustrando métodos y aparatos conforme a algunas implementaciones en relación a la personalización de seguridad de una aplicación software de dispositivo móvil. En particular, la figura 1 ilustra un método asociado con uno o más proveedores de servicios (201, 202, 203 and 204) y un proveedor de servicios de personalización (100) en relación a la personalización de seguridad de una aplicación software de dispositivo móvil en un dispositivo móvil de un usuario (400).

La aplicación software de dispositivo móvil puede ser desarrollada de tal forma que partes de ella puedan realizar funciones asociadas a uno o más proveedores de servicios, otras partes puedan realizar funciones asociadas a otros uno o más proveedores de servicios, etc. También, diferentes partes de la aplicación software de dispositivo móvil constituyen diferentes dominios de código, cada uno agrupando una o más funciones de la aplicación software de dispositivo móvil que están asociadas a uno o más proveedores de servicios.

En esta invención se aplica personalización de seguridad a ciertos dominios de código, dicha personalización habilitándolos para operación regular, es decir que los habilita para realizar regularmente las funciones del dominio de código asociadas a los uno o más proveedores de servicios relacionados. Algunas de esas funciones pueden ser relativas a procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil tales como procesos de registro de servicios, procesos de personalización, procesos de pago, procesos de autenticación, solicitudes de información, etc., tal y como se ilustra en la figura 1.

En consecuencia, algunos procesos pueden tener lugar entre el dispositivo móvil del usuario y un servidor de registro de servicios, un servidor de personalización, un terminal de transacciones, un servidor de autenticación, un terminal proxy, un servidor proxy, un servidor procesando una primera parte de una transacción, un servidor procesando procesos de ciclo de vida de aplicación, etc. Otras funciones pueden ser relativas por ejemplo a procesos locales realizados por la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario.

En la figura 1 se ilustran varios proveedores de servicios, particularmente el proveedor de servicios 1 (201), el proveedor de servicios 2 (202), el proveedor de servicios 3 (203) y el proveedor de servicios 4 (204). Los proveedores de servicios pueden ser autoridades de transporte, empresas de servicios de salud, proveedores de servicios de internet de las cosas, proveedores de servicios de localización y/o presencia, instituciones financieras, etc.

Conforme a algunas implementaciones el proveedor de servicios de personalización es uno de los uno o más proveedores de servicios. En un ejemplo particular el proveedor de servicios 1 es la misma entidad que el proveedor de servicios de personalización y los dominios de código y las funciones relativas en una aplicación software de dispositivo móvil están enteramente asociadas al proveedor de servicios 1.

En el paso (1) uno o más dispositivos de procesamiento dentro del sistema del proveedor de servicios de personalización genera un conjunto de registros de personalización de seguridad y los almacena en una base de datos (BD) asociada a aplicaciones software protegidas de dispositivo móvil. Conforme a algunas implementaciones al menos parte de los registros de personalización de seguridad son generados a partir de datos de entrada proporcionados al proveedor de servicios de personalización por uno o más proveedores de servicios (esta posibilidad es representada en la figura 1 como paso (0) y paso (0´), en referencia al proveedor de servicios 1 y al proveedor de servicios 3 respectivamente, donde los datos de entrada son recibidos en el módulo de personalización de seguridad) tal que el proveedor de servicios relacionado pueda después asociar una al menos parte de un registro de personalización de seguridad recibido desde el proveedor de servicios de personalización con los datos de entrada relacionados.

La figura 1 ilustra un ejemplo de registros de personalización de seguridad generados de la siguiente forma:

- un registro de personalización de seguridad de inicialización (RPS-I) que incluye un conjunto de subregistros de seguridad genérica RS_1, RS_2, RS_3, SR_4, …, RS_i, …, RS_n, y un conjunto de subregistros de personalización de seguridad RPS_{21}, RPS_{31}, RPS_{41}, …, RPS_{i1}, …, RPS_{n1};

- un conjunto de registros de personalización de seguridad de ciclo de vida adicionales asociados a los subregistros de seguridad genérica RS_1 y RS_2: RPS_{22}, RPS_{23}, …, RPS_{2j}, …, RPS_{2N}];

- un conjunto de registros de personalización de seguridad de ciclo de vida adicionales asociados a los subregistros de seguridad genérica RS_1 y RS_3: RPS_{32}, RPS_{33}, …, RPS_{3j}, …, RPS_{3N}];

- un conjunto de registros de personalización de seguridad de ciclo de vida adicionales asociados a los subregistros de seguridad genérica RS_1 y RS_4: [RPS_{42}, RPS_{43}, …, RPS_{4j}, …, RPS_{4N}];

- un conjunto de registros de personalización de seguridad de ciclo de vida adicionales asociados a los subregistros de seguridad genérica RS_1 y RS_i: [RPS_{i2}, RPS_{i3}, …, RPS_{ij}, …, RPS_{iN}];

- un conjunto de registros de personalización de seguridad de ciclo de vida adicionales asociados a los subregistros de seguridad genérica RS_1 y RS_n: [RPS_{n2}, RPS_{n3}, …, RPS_{nj}, …, RPS_{nN}];

En el paso (2) el proveedor de servicios de personalización utiliza una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad que están almacenados en una o más memorias para generar utilizando uno o más dispositivos de procesamiento una aplicación software protegida de dispositivo móvil que está personalizada en términos de seguridad utilizando datos del registro de personalización de seguridad. En un ejemplo particular el registro de personalización de seguridad es el registro de personalización de seguridad de inicialización (RPS-I) referido anteriormente.

Conforme a algunas implementaciones las una o más memorias y los uno o más dispositivos de procesamiento residen en uno o más servidores del proveedor de servicios de personalización.

Tal y como se ha descrito anteriormente la aplicación generada incluye varios dominios de código, relativos a los uno o más proveedores de servicios, donde uno o más primeros dominios de código están vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar los uno o más primeros dominios de código para operación regular.

La aplicación puede ser testeada con objeto de verificar que la personalización de seguridad habilita los uno o más dominios de código para operación regular (ej. usando un emulador de dispositivo móvil que sea parte del software de protección de seguridad). En el paso (3) la aplicación software protegida de dispositivo móvil es almacenada en la base de datos (BD) asociada a aplicaciones software protegidas de dispositivo móvil, en relación a los datos de personalización de seguridad que habilitan los uno o más primeros dominios de código para operación regular y a los registros de personalización de seguridad (incluyendo RPS-I)

Posteriormente, en el paso (4) el módulo de personalización de seguridad obtiene usando uno o más dispositivos de procesamiento la aplicación software protegida de dispositivo móvil de la base de datos.

Conforme a algunas implementaciones la aplicación protegida es obtenida sin ningún dato asociado a la personalización de seguridad que habilita los uno o más primeros dominios de código para operación regular, por lo que la aplicación obtenida es una aplicación software protegida de dispositivo móvil no personalizada en seguridad. La aplicación software protegida de dispositivo móvil no personalizada en seguridad está en un estado de personalización de seguridad pendiente, dicho estado de personalización de seguridad pendiente deshabilitando los uno o más primeros dominios de código para operación regular.

En el paso (5) la aplicación software protegida de dispositivo móvil es enviada en un estado de seguridad no-personalizada desde el proveedor de servicios de personalización a un servidor de distribución de una entidad a cargo de distribuir la aplicación y dicha aplicación es almacenada en una o más memorias del servidor de distribución de dicha entidad. Como se ilustra en la figura 1, conforme a algunas implementaciones el servidor de distribución es relativo a uno o más de los servidores asociados a un mercado de distribución de aplicaciones o a una tienda de aplicaciones tales como Google Play Store o Apple Store.

En el paso (6) tras una interacción por parte del usuario (300) hay una solicitud desde el dispositivo móvil del usuario de una aplicación software de dispositivo móvil al servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada. Como puede ser bien entendido por aquellos expertos en la técnica, otros servidores pueden estar involucrados en recibir la solicitud desde el dispositivo móvil del usuario y/o en distribuir la aplicación al dispositivo móvil del usuario, pero independientemente de la arquitectura de servidores de la entidad que distribuye aplicaciones a dispositivos móviles, la solicitud de esta invención esta orientada a obtener la aplicación software protegida de dispositivo móvil no personalizada en seguridad desde el referido servidor de distribución, para distribución al dispositivo móvil del usuario.

En el paso (7) el dispositivo móvil del usuario recibe desde el servidor de distribución y a continuación instala mediante una o más dispositivos de procesamiento en el dispositivo móvil la aplicación software protegida de

dispositivo móvil no personalizada en seguridad, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código están deshabilitados para operación regular.

Como se describe a continuación, conforme a algunas implementaciones el dispositivo móvil del usuario se usa en relación a la personalización de seguridad de la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario.

En el paso (8) el dispositivo móvil del usuario envía una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada.

En el paso (9) el proveedor de servicios de personalización recibe la solicitud desde el dispositivo móvil del usuario y en el paso (10) uno o más dispositivos de procesamiento del proveedor de servicios de personalización asigna un registro de personalización de seguridad de ciclo de vida al dispositivo móvil del usuario en relación a la aplicación software protegida de dispositivo móvil. Conforme a algunas implementaciones el registro de personalización de seguridad de ciclo de vida asignado en este paso por el módulo de personalización de seguridad es diferente (ej. RPS33) que el registro de personalización de seguridad usado cuando se generó la aplicación software de dispositivo móvil personalizada en seguridad (RPS-I en el ejemplo de arriba). Todavía en el paso (10) la asignación del registro de personalización de seguridad de ciclo de vida al dispositivo móvil del usuario y a la aplicación software protegida de dispositivo móvil es almacenada en la base de datos asociada a aplicaciones software protegidas de dispositivo móvil.

En el paso (11) al menos parte de los datos del registro de personalización de seguridad de ciclo de vida asignado, y la asociación al dispositivo móvil del usuario y a la aplicación software protegida de dispositivo móvil, puede ser enviada al proveedor de servicios correspondiente tal que este pueda posteriormente usar al menos parte de estos en el contexto de ciertos procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil (la figura 1 ilustra un ejemplo donde dichos datos son enviados al proveedor de servicios 1).

En el paso (12) datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida asignado son enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario. En particular, datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario son enviados a la aplicación software protegida de dispositivo móvil no personalizada en seguridad en el dispositivo móvil del usuario, los datos de personalización de seguridad habilitando en la aplicación al menos uno de los uno o más primeros dominios de código para operación regular.

En el paso (13) el dispositivo móvil del usuario recibe los datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, lo datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones el habilitado de el al menos uno de los uno o más primeros dominios de código está asociado a uno o más parámetros de seguridad relativos al registro de personalización de seguridad de ciclo de vida, que son diferentes que los correspondientes del registro de personalización de seguridad.

Ventajosamente, después de que la personalización de seguridad anterior haya sido realizada, los referidos al menos uno de los uno o más primeros dominios de código pueden ser usados para realizar regularmente las funciones asociadas de ciclo de vida de la aplicación software protegida de dispositivo móvil.

Conforme a algunas implementaciones diferentes grupos de uno o más primeros dominios de Código no-habilitados son personalizados en términos de seguridad en diferentes instantes temporales. Esta aproximación incrementa la seguridad de la aplicación software protegida de dispositivo móvil. Los pasos (14a, 15a y 16a) representan solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código, enviadas desde el dispositivo móvil del usuario al proveedor de servicios de personalización.

Dentro de estas implementaciones, cada solicitud del dispositivo móvil del usuario es lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular.

En el paso (14a) una solicitud sucesiva es enviada desde el dispositivo móvil del usuario al proveedor de servicios de personalización y en el paso (14b) el proveedor de servicios de personalización recibe la solicitud sucesiva desde el dispositivo móvil del usuario, y uno o más dispositivos de procesamiento del proveedor de servicios de personalización obtiene en el paso (14c) datos de personalización de seguridad del registro de personalización de seguridad de ciclo de vida previamente asignado al dispositivo móvil del usuario.

En el paso (14d) los datos de personalización de seguridad del registro de personalización de seguridad de ciclo de vida previamente asignado al dispositivo móvil del usuario son enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario. En particular, datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida son enviados a la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad.

En el paso (14e) el dispositivo móvil del usuario recibe del proveedor de servicios de personalización los datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

Los procesos asociados a los pasos 15b, 15c, 15d y 15e serán similares a aquellos ya descritos en relación a 14a, 14b, 14c, 14d y 14e, pero ahora en relación a la solicitud sucesiva 15a y a la habilitación en la aplicación para operación regular de el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular (15a).

También, los procesos asociados a los pasos 16b, 16c, 16d y 16e serán similares a aquellos ya descritos arriba en relación a 14a, 14b, 14c, 14d y 14e (o a 15a, 15b, 15c, 15d y 15e) pero ahora en relación a la solicitud sucesiva 16a y a la habilitación en la aplicación para operación regular de el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular (16a).

Conforme a algunas implementaciones al menos uno del otro uno o más primeros dominios de código está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular. Más allá, conforme a algunas implementaciones al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados a una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a los uno o más primeros dominios de código.

Una vez que los datos de personalización de seguridad son recibidos y almacenados en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, el al menos uno del otro uno o más primeros dominios de código queda vinculado en la aplicación en términos de seguridad al uno o más primeros dominios de código mediante dicha personalización de seguridad que es relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular. Conforme a algunas implementaciones dichos parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código han sido recibidos en la aplicación y están disponibles en una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a uno o más primeros dominios de código que han sido previamente habilitados para operación regular.

Conforme a algunas implementaciones uno o más dispositivos de procesamiento en el sistema del proveedor de servicios de personalización hacen una aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad expirar si una solicitud para una personalización de seguridad de al menos otro uno o más primeros dominios de código es recibida más tarde que un periodo de tiempo predefinido después de que datos de personalización de seguridad relativos a una solicitud previa para una personalización de seguridad de al menos uno u otro diferente uno de los uno o más primeros dominios de código fueran enviados

a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada o parcialmente-personalizada. Esta aproximación aumenta aún más la seguridad de la aplicación software protegida de dispositivo móvil.

Conforme a algunas implementaciones, una notificación desde el proveedor de servicios de personalización indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado es enviada al dispositivo móvil del usuario y recibida en el dispositivo móvil del usuario.

En un ejemplo particular los procesos incluyendo hasta el paso 13 ya han sido realizados por lo que la aplicación software protegida de dispositivo móvil está en un estado de seguridad parcialmente personalizada. Como se ha descrito anteriormente, en el paso (14a) una solicitud sucesiva es enviada desde el dispositivo móvil del usuario y recibida en el paso (14b) por el proveedor de servicios de personalización. Dentro de este ejemplo, en el paso (14c), previamente a obtener datos de personalización de seguridad del registro de personalización de seguridad de ciclo de vida previamente asignado al dispositivo móvil del usuario, uno o más dispositivos de procesamiento del proveedor de servicios de personalización verifican si la solicitud ha sido recibida (paso 14b) más tarde que un periodo de tiempo predefinido después de que datos de personalización de seguridad fueran enviados a la aplicación software protegida de dispositivo móvil en el paso (12).

Si la solicitud ha sido recibida más tarde que dicho periodo de tiempo predefinido, entonces la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad asociada al dispositivo móvil del usuario expira en el sistema del proveedor de servicios de personalización. Conforme a algunas implementaciones, el proveedor de servicios de personalización notifica (no ilustrado en la figura 1) a uno o más proveedores de servicios acerca del estado de expiración de la aplicación software protegida de dispositivo móvil asociada al dispositivo móvil del usuario. También, una notificación indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado es enviada al dispositivo móvil del usuario y recibida en el dispositivo móvil del usuario.

En otro ejemplo particular los procesos incluyendo hasta el paso 14e ya han sido realizados por lo que la aplicación software protegida de dispositivo móvil está en un estado de seguridad parcialmente personalizada. En el paso (15a) una solicitud sucesiva es enviada desde el dispositivo móvil del usuario y recibida en el paso (15b) por el proveedor de servicios de personalización. Dentro de este ejemplo, en el paso (15c), previamente a obtener datos de personalización de seguridad del registro de personalización de seguridad de ciclo de vida previamente asignado al dispositivo móvil del usuario, uno o más dispositivos de procesamiento del proveedor de servicios de personalización verifican si la solicitud ha sido recibida (paso 15b) más tarde que un periodo de tiempo predefinido después de que datos de personalización de seguridad fueran enviados a la aplicación software protegida de dispositivo móvil en el paso (14d).

Si la solicitud ha sido recibida más tarde que dicho periodo de tiempo predefinido, entonces la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad asociada al dispositivo móvil del usuario expira en el sistema del proveedor de servicios de personalización. Conforme a algunas implementaciones, el proveedor de servicios de personalización notifica (no ilustrado en la figura 1) a uno o más proveedores de servicios acerca del estado de expiración de la aplicación software protegida de dispositivo móvil asociada al dispositivo móvil del usuario. Complementariamente, una notificación indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado puede ser enviada al dispositivo móvil del usuario.

Conforme a algunas implementaciones los uno o más primeros/segundos dominios de código asociados en una o más memorias del proveedor de servicios de personalización a la aplicación software protegida de dispositivo móvil en un dispositivo móvil de un primer usuario son diferentes que los uno o más primeros/segundos dominios de código asociados en una o más memorias del proveedor de servicios de personalización a la aplicación software protegida de dispositivo móvil en un dispositivo móvil de un segundo usuario. En una implementación particular cada registro de personalización de seguridad de ciclo de vida está ya asociado a un conjunto de uno o más primeros y segundos dominios de código en la fase de generación (en un ejemplo particular: RPS33 está asociado a los dominios de código 1, 3/1 and 3/2; y RPS42 está asociado a los dominios de código 1, 4/1 and 4/2) tal que cuando un registro de personalización de seguridad de ciclo de vida es asignado a un dispositivo móvil de un usuario dado en el paso (10) la asociación al correspondiente conjunto de uno o más primeros y segundos dominios de código es heredada.

Conforme a algunas implementaciones el uno o más primeros dominios de código habilitados mediante primeros datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un primer usuario son diferentes que los uno o más primeros dominios de

código habilitados mediante segundos datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un segundo usuario.

Conforme a algunas implementaciones los datos de personalización de seguridad recibidos en el dispositivo móvil de un primer usuario,

Conforme a algunas implementaciones los datos de personalización de seguridad recibidos en el dispositivo móvil de un primer usuario, los datos habilitando en la aplicación uno o más primeros dominios de código para operación regular y asociados a un primer registro de personalización de seguridad de ciclo de vida que incluye primeros parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código, son diferentes que los datos de personalización de seguridad recibidos en el dispositivo móvil de un segundo usuario, los datos habilitando en la aplicación uno o más primeros dominios de código para operación regular y asociados a un segundo registro de personalización de seguridad de ciclo de vida que incluye segundos parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código.

Conforme a algunas implementaciones la aplicación software protegida de dispositivo móvil puede ser re personalizada a lo largo de su ciclo de vida.

La figura 1 ilustra una implementación en donde uno o más dispositivos de procesamiento dentro del sistema del proveedor de servicios de personalización obtiene en el paso (17) datos de re personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida, o a otro registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario, desde la base de datos asociada a la aplicación software protegida de dispositivo móvil.

Los referidos datos de re personalización de seguridad son enviados en el paso (18) a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad parcialmente personalizada o personalizada, los datos de re personalización de seguridad son al menos parcialmente diferentes que los datos de personalización de seguridad.

En el paso (19) los datos de re personalización de seguridad son recibidos en la aplicación software protegida de dispositivo móvil estando en un estado de seguridad parcialmente personalizada o personalizada, y habilitan en la aplicación para operación regular al menos uno de los uno o más primeros dominios de código y/o al menos uno del otro uno o más primeros dominios de código. Ventajosamente, en esta invención al menos parte de la protección de seguridad puede ser renovada de vez en cuando a bajo ciertas circunstancias.

Conforme a algunas implementaciones al menos uno del otro uno o más primeros dominios de código está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código a través de la re personalización de seguridad, dicha re personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en el uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular. Adicionalmente, conforme a algunas implementaciones al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados a una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a los uno o más primeros dominios de código.

Las figuras 2.a a 2.l son diagramas esquemáticos ilustrando métodos y aparatos conforme a algunas implementaciones en relación a la personalización de seguridad de una aplicación software de dispositivo móvil. Por simplicidad, estos diagramas ilustran métodos asociados con un proveedor de servicios y un proveedor de servicios de personalización en relación a la personalización de seguridad de una aplicación software de dispositivo móvil en un dispositivo móvil de un usuario. Para mayor simplicidad, en la descripción de estos diagramas se considerará que el proveedor de servicios y el proveedor de servicios de personalización son la misma entidad (proveedor de servicios 1 en el contexto de las figuras 2.a a 2.l).

La figura 2.a ilustra un ejemplo de registros de personalización de seguridad generados por el proveedor de servicios de personalización. Como ya se ha referido en relación al paso (1) de la figura 1, uno o más dispositivos de procesamiento dentro del sistema del proveedor de servicios de personalización genera un conjunto de registros de personalización de seguridad.

En el ejemplo ilustrado en la figura 2.a hay un registro de personalización de seguridad de inicialización (RPS-I) que incluye un conjunto de subregistros de seguridad genérica RS_1, RS_2, RS_3, RS_4, …, RS_i, …, RS_n, y un conjunto de subregistros de personalización de seguridad RPS_{21}, RPS_{31}, RPS_{41}, …, RPS_{i1}, …, RPS_{n1} donde:

- RS_1 and RS_2 are associated to RPS_{21};
- RS_1 and RS_3 are associated to RPS_{31};
- RS_1 and RS_4 are associated to RPS_{41};
- RS_1 and RS_i are associated to RPS_{i1};
- RS_1 and RS_n are associated to RPS_{n1};

Dentro de este ejemplo los subregistros de seguridad genérica y los subregistros de personalización de seguridad incluyen datos asociados a parámetros de seguridad (ps), reglas de ofuscación (ro) y redes de checksums (ch). En otro ejemplo particular los subregistros de personalización de seguridad incluyen datos asociados a parámetros de seguridad (ps) y/o reglas de ofuscación (ro) y/o redes de checksums (ch).

La figura 2.a también ilustra diferentes conjuntos de registros de personalización de seguridad de ciclo de vida adicionales de la siguiente forma:

- un conjunto de registros de personalización de seguridad de ciclo de vida asociados a los subregistros de seguridad genérica RS_1 y RS_2: RPS_{22}, RPS_{23}, …, RPS_{2j}, …, RPS_{2N}];
- un conjunto de registros de personalización de seguridad de ciclo de vida asociados a los subregistros de seguridad genérica RS_1 y RS_3: RPS_{32}, RPS_{33}, …, RPS_{3j}, …, RPS_{3N}];
- un conjunto de registros de personalización de seguridad de ciclo de vida asociados a los subregistros de seguridad genérica RS_1 y RS_4: RPS_{42}, RPS_{43}, …, RPS_{4j}, …, RPS_{4N}];
- un conjunto de registros de personalización de seguridad de ciclo de vida asociados a los subregistros de seguridad genérica RS_1 y RS_i: RPS_{i2}, RPS_{i3}, …, RPS_{ij}, …, RPS_{iN}];
- un conjunto de registros de personalización de seguridad de ciclo de vida asociados a los subregistros de seguridad genérica RS_1 y RS_n: RPS_{n2}, RPS_{n3}, …, RPS_{nj}, …, RPS_{nN}];

Dentro de este ejemplo los registros de personalización de seguridad de ciclo de vida incluyen datos asociados a parámetros de seguridad (ps), reglas de ofuscación (ro) y redes de checksums (ch). En otro ejemplo particular los registros de personalización de seguridad de ciclo de vida incluyen datos asociados a parámetros de seguridad (ps) y/o reglas de ofuscación (ro) y/o redes de checksums (ch).

La figura 1 ilustra el uso por el proveedor de servicios de personalización de una aplicación software de dispositivo móvil, un registro de personalización de seguridad (RPS-I en el ejemplo de la figura 1) y software de protección de seguridad para generar una aplicación software protegida de dispositivo móvil que está personalizada en términos de seguridad utilizando datos del registro de personalización de seguridad.

Conforme a algunas implementaciones se calculan parámetros de seguridad dentro del sistema del proveedor de servicios de personalización. En un ejemplo particular los parámetros de seguridad son calculados en el módulo de personalización de seguridad y son almacenados en los registros de personalización de seguridad. La figura 2.a ilustra los parámetros de seguridad (ps) calculados almacenados en los correspondientes registros de personalización de seguridad (RPS-I, RPS_{22}, … , RPS_{2N}, … , RPS_{nN})

Conforme a algunas implementaciones parámetros de seguridad del registro de personalización de seguridad (RPS-I en el ejemplo) son usados por el software de protección de seguridad para proteger ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones al menos parte de los parámetros de seguridad del registro de personalización de seguridad son embebidos por el software de protección de seguridad en el código de aplicación (ej. $ps_{3\text{-}RS1}$). Conforme a algunas implementaciones, parte de al menos un parámetro de seguridad dado del registro de personalización de seguridad es embebido por el software de protección de seguridad en el código de aplicación (ej. $ps_{1a\text{-}RS2}$) y otra parte es almacenada en la base de datos de la aplicación software protegida de dispositivo móvil (ej. $ps_{1b\text{-}RPS21}$).

Conforme a algunas implementaciones al menos parte de los parámetros de seguridad del registro de personalización de seguridad (RPS-I en el ejemplo) son ofuscados por el software de protección de seguridad en el código de la aplicación software de dispositivo móvil (ej. $ps_{3\text{-}RS1}$), usando reglas de ofuscación incluidas en el registro de personalización de seguridad (ej. $ro_{3\text{-}RS1}$). Conforme a algunas implementaciones, parte de al menos un parámetro de seguridad dado del registro de personalización de seguridad es ofuscado por el software de protección de seguridad en el código de aplicación (ej. $ps_{1a\text{-}RS2}$) y otra parte es almacenada en un formato ofuscado en la base de datos de la aplicación software protegida de dispositivo móvil (ej. $ps_{1b\text{-}RPS21}$), usando reglas de ofuscación incluidas en el registro de personalización de seguridad (ej. una parte de $ro_{3\text{-}RS1}$ y $ro_{1b\text{-}RPS21}$).

Conforme a algunas implementaciones una aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un usuario es personalizada con al menos parte de al menos un parámetro de seguridad dado, dicha parte incluida en un registro de personalización de seguridad de ciclo de vida (ej. $ps_{1b\text{-}RPS33}$ incluido en RPS_{33}) y siendo almacenada durante un proceso de personalización de seguridad en la base de datos de la aplicación software protegida de dispositivo móvil, el parámetro de seguridad protegiendo ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones al menos parte de al menos un parámetro de seguridad dado, dicha parte incluida en un registro de personalización de seguridad de ciclo de vida (ej. $ps_{1b\text{-}RPS33}$ incluido en RPS_{33}), es almacenada durante un proceso de personalización de seguridad en un formato ofuscado en la base de datos de una aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un usuario, usando reglas de ofuscación que están parcialmente incluidas en el registro de personalización de seguridad (ej. parte de $ro_{3\text{-}RS1}$) y parcialmente incluidas en el registro de personalización de seguridad de ciclo de vida (ej. parte de $ro_{1b\text{-}RPS33}$), el parámetro de seguridad protegiendo ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones redes de checksums son calculadas dentro de sistema del proveedor de servicios de personalización. En un ejemplo particular las redes de checksums son calculadas por el software de protección de seguridad y son almacenadas en los registros de personalización de seguridad. La figura 2.a ilustra las redes de checksums (ch) calculadas almacenadas en los correspondientes registros de personalización de seguridad (RPS-I, RPS_{22}, … , RPS_{2N}, … , RPS_{nN}).

Conforme a algunas implementaciones al menos parte de los checksums de las redes de checksums del registro de personalización de seguridad (RPS-I en el ejemplo) son calculados como checksums del código de aplicación (ej. $ch_{3\text{-}RS1}$). Conforme a algunas implementaciones al menos parte de los checksums de las redes de checksums del registro de personalización de seguridad son calculados como checksums del código de la aplicación y/o de parámetros de seguridad del registro de personalización de seguridad (ej. $ch_{3\text{-}RS2}$ calculado usando una parte dada del código de la aplicación y $ps_{5\text{-}RS1}$; o ej. $ch_{1b\text{-}RPS21}$ calculado usando $ps_{3\text{-}RS2}$; o ej. $ch_{1b\text{-}RPS21}$ calculado usando $ps_{1b\text{-}RPS21}$).

Conforme a algunas implementaciones redes de checksums del registro de personalización de seguridad (RPS-I en el ejemplo) son usadas por el software de protección de seguridad para proteger ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones al menos parte de las redes de checksums del registro de personalización de seguridad son embebidas por el software de protección de seguridad en el código de la aplicación (ej. $ch_{3\text{-}RS1}$). Conforme a algunas implementaciones, parte de al menos un checksum dado del registro de personalización de seguridad es embebido por el software de protección de seguridad en el código de la aplicación (ej. $ch_{1a\text{-}RS2}$) y otra parte es almacenada en la base de datos de la aplicación software protegida de dispositivo móvil (ej. $ch_{1b\text{-}RPS21}$).

Conforme a algunas implementaciones al menos parte de las redes de checksums del registro de personalización de seguridad (RPS-I en el ejemplo) son ofuscadas por el software de protección de seguridad dentro del código de la aplicación software de dispositivo móvil (ej. $ch_{3\text{-}RS1}$), usando reglas de ofuscación incluidas en el registro de personalización de seguridad (ej. $ro_{3\text{-}RS1}$). Conforme a algunas implementaciones, parte de al menos un checksum dado del registro de personalización de seguridad es ofuscada por el software de protección de seguridad en el código de la aplicación (ej. $ch_{1a\text{-}RS2}$) y otra parte es almacenada en un formato ofuscado en la base de datos de la aplicación software protegida de dispositivo móvil (ej. $ch_{1b\text{-}RPS21}$), usando reglas de ofuscación incluidas en el registro de personalización de seguridad (ej. una parte de $ro_{3\text{-}RS1}$ and $ro_{1b\text{-}RPS21}$).

Conforme a algunas implementaciones una aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un usuario es personalizada con al menos parte de al menos un checksum dado, dicha parte incluida en un registro de personalización de seguridad de ciclo de vida (ej. $ch_{1b\text{-}RPS33}$ incluido en RPS_{33}) y siendo almacenada durante un proceso de personalización de seguridad en la base de datos de la aplicación software protegida de dispositivo móvil, el checksum protegiendo ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones al menos parte de al menos un checksum dado, dicha parte incluida en un registro de personalización de seguridad de ciclo de vida (ej. $ch_{1b\text{-}RPS33}$ incluido en RPS_{33}), es almacenado durante un proceso de personalización de seguridad en un formato ofuscado en la base de datos de una aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un usuario, usando reglas de ofuscación que están parcialmente incluidas en el registro de personalización de seguridad (ej. $ro_{3\text{-}RS1}$) y parcialmente incluidas en el registro de personalización de seguridad de ciclo de vida ($ro_{1b\text{-}RPS33}$), el checksum protegiendo ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones un proceso de ofuscación es aplicado dentro del sistema del proveedor de servicios de personalización al código de la aplicación, y/o a parámetros de seguridad del registro de personalización de seguridad que están al menos parcialmente embebidos en el código de la aplicación y/o que está parcialmente almacenados en la base de datos de la aplicación, y/o a checksums de las redes de checksums del registro de personalización de seguridad que están al menos parcialmente embebidos en el código de la aplicación y/o que están al menos parcialmente almacenados en la base de datos de la aplicación. En un ejemplo particular el referido proceso de ofuscación es aplicado por el software de protección de seguridad.

El proceso de ofuscación puede incluir una diversidad de técnicas de ofuscación bien conocidas tales como por ejemplo reemplazar una instrucción del código de la aplicación o un conjunto de instrucciones del código de aplicación con otra instrucción de código de aplicación o conjunto de instrucciones de aplicación con funcionalidad equivalente; cambiar el orden de instrucciones del código de la aplicación; cambiar el orden de funciones o bloques de instrucciones del código de la aplicación; cambiar la estructura de bucles; añadir saltos sin sentido; insertar datos o instrucciones de código de aplicación sin uso; entrelazar una o más secuencias de código de la aplicación; reordenar datos estáticos; reordenación de datos de tiempo de ejecución; encriptación de instrucciones de programa; encriptación de datos estáticos; reemplazar valores constantes con código de aplicación que genera el valor constante; mover datos estáticos o de tiempo de ejecución entre pilas, montones y registros; usar diferentes pilas; usar varios punteros de pila para la misma pila; hacer que el código de programa se auto modifique; mezclar datos (ej. parámetros de seguridad y/ checksums del código) con código de programa; asignar particiones de datos de seguridad, embebidas en diferentes partes del código de la aplicación; renombrar clases, funciones, o variables; renombrar ficheros o módulos. Como puede ser bien entendido por un experto en la técnica, la lista anterior no es exhaustiva y otras técnicas de ofuscación adicionales pueden ser también aplicadas a la aplicación software de dispositivo móvil sin alejarse del ámbito de esta invención. También, debe ser entendido que algunas de las técnicas pueden ser aplicadas más de una vez (eso es aplicar una o más técnicas de ofuscación a código y/o datos ya ofuscados) para conseguir un grado de ofuscación mayor.

Conforme a algunas implementaciones el proceso de ofuscación depende de un paso previo de calcular reglas de ofuscación del registro de personalización de seguridad (RPS-I en el ejemplo) que son usadas por el software de protección de seguridad para proteger ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones reglas de ofuscación son calculadas en el sistema del proveedor de servicios de personalización y son almacenadas en los registros de personalización de seguridad. En un ejemplo particular las reglas de ofuscación son calculadas por el software de protección de seguridad o en el módulo de personalización de seguridad. La figura 2.a ilustra las reglas de ofuscación (ro) calculadas almacenadas en los correspondientes registros de personalización de seguridad (RPS-I, RPS_{22}, … , RPS_{2N}, … , RPS_{nN}).

Conforme a algunas implementaciones al menos parte de las reglas de ofuscación del registro de personalización de seguridad (RPS-I en el ejemplo) son calculadas en relación a la ofuscación del código de la aplicación (ej. $ro_{3\text{-}RS1}$ calculado en relación a la ofuscación de una parte dada del código de la aplicación). Conforme a algunas implementaciones al menos parte de las reglas de ofuscación del registro de personalización de seguridad son calculadas en relación a la ofuscación del código de la aplicación y/o de parámetros de seguridad del registro de personalización de seguridad que están al menos al menos parcialmente embebidos en el código de la aplicación y/o que están al menos parcialmente almacenados en la base de datos de la aplicación, y/o de checksums de las redes de checksums del registro de personalización

de seguridad que están al menos parcialmente embebidos en el código de la aplicación y/o que están al menos parcialmente almacenados en la base de datos de la aplicación (ej. $ro_{3\text{-}RS1}$ calculada en relación a la ofuscación de una parte dada del código de la aplicación y a la ofuscación de $ps_{3\text{-}RS2}$ y a la ofuscación de $ch_{3\text{-}RS2}$; o ej. $ro_{1b\text{-}RPS31}$ calculada en relación a la ofuscación de $ps_{1b\text{-}RPS31}$ y $ch_{1b\text{-}RPS31}$).

Conforme a algunas implementaciones al menos parte de las reglas de ofuscación del registro de personalización de seguridad son embebidas por el software de protección de seguridad en el código de la aplicación (ej. $ro_{1\text{-}RS1}$) durante un proceso de ofuscación. Conforme a algunas implementaciones, durante un proceso de ofuscación parte de al menos una regla de ofuscación dada del registro de personalización de seguridad es embebida por el software de protección de seguridad en el código de la aplicación (ej. $ro_{1a\text{-}RS4}$) y otra parte es almacenada en la base de datos de la aplicación software protegida de dispositivo móvil (ej. $ro_{1b\text{-}RPS41}$). Conforme a algunas implementaciones, la aplicación software protegida de dispositivo móvil es programada para usar al menos parte de las reglas de ofuscación embebidas/almacenadas para ejecutar correctamente instrucciones de código de la aplicación y/o para obtener/usar datos de la aplicación según definido.

Conforme a algunas implementaciones al menos parte de las reglas de ofuscación del registro de personalización de seguridad (RPS-I en el ejemplo) están ofuscadas en relación a otras reglas de ofuscación (ej. $ro_{1b\text{-}RPS41}$ ofuscada en la aplicación software protegida de dispositivo móvil en relación a $ro_{m\text{-}RS1}$).

Conforme a algunas implementaciones una aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un usuario es personalizada con al menos parte de al menos una regla de ofuscación dada, dicha parte incluida en un registro de personalización de seguridad de ciclo de vida (ej. $ro_{1b\text{-}RPS33}$ incluida en RPS_{33}) y siendo almacenada durante un proceso de personalización de seguridad en la base de datos de la aplicación software protegida de dispositivo móvil, la regla de ofuscación protegiendo ciertos datos sensibles y/o procesos de / asociados a la aplicación software de dispositivo móvil.

Conforme a algunas implementaciones parte de al menos una regla de ofuscación dada, dicha parte incluida en un registro de personalización de seguridad de ciclo de vida (ej. $ro_{2b\text{-}RPS33}$ incluida en RPS_{33}), es almacenada durante un proceso de personalización de seguridad en un formato ofuscado en la base de datos de una aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un usuario, usando para la ofuscación al menos parte de otra regla de ofuscación dada (ej. $ro_{2b\text{-}RPS33}$ ofuscada usando al menos parte de $ro_{1a\text{-}RS3}$ and $ro_{1b\text{-}RPS33}$).

La figura 2.b es relativa a algunas implementaciones donde una aplicación software de dispositivo móvil ha sido desarrollada para realizar funciones asociadas a un proveedor de servicios (proveedor de servicios 1 en el contexto de 2.a a 2.l) que es la misma entidad que el proveedor de servicios de personalización.

Conforme a algunas implementaciones, diferentes partes de la aplicación software de dispositivo móvil constituyen diferentes dominios de código, cada una agrupando una o más funciones de la aplicación software de dispositivo móvil que están asociadas al proveedor de servicios. La figura 2.b ilustra un ejemplo de una aplicación software de dispositivo móvil con los siguientes dominios de código y funciones asociadas al proveedor de servicios:

- Dominio de código 1 (DC1) incluyendo funciones ($f1_{DC1}$, $f2_{DC1,}$ …) de la aplicación software de dispositivo móvil;
- Dominio de código 2/1 (DC2/1) incluyendo funciones ($f1_{DC2/1}$, $f2_{DC2/1,}$ …) de la aplicación software de dispositivo móvil;
- Dominio de código 2/2 (DC2/2) incluyendo funciones ($f1_{DC2/2}$, $f2_{DC2/2,}$ …) de la aplicación software de dispositivo móvil;
- Dominio de código 3/1 (DC3/1) incluyendo funciones ($f1_{DC3/1}$, $f2_{DC3/1,}$ …) de la aplicación software de dispositivo móvil;
- Dominio de código 3/2 (DC3/2) incluyendo funciones ($f1_{DC3/2}$, $f2_{DC3/2,}$ …) de la aplicación software de dispositivo móvil;
- Dominio de código 4/1 (DC4/1) incluyendo funciones ($f1_{DC4/1}$, $f2_{DC4/1,}$ …) de la aplicación software de dispositivo móvil;

- Dominio de código 4/2 (DC4/2) incluyendo funciones ($f1_{DC4/2}$, $f2_{DC4/2,}$ …) de la aplicación software de dispositivo móvil;

- Dominio de código i/1 (DCi/1) incluyendo funciones ($f1_{DCi/1}$, $f2_{DCi/1,}$ …) de la aplicación software de dispositivo móvil;

- Dominio de código i/2 (DCi/2) incluyendo funciones ($f1_{DCi/2}$, $f2_{DCi/2,}$ …) de la aplicación software de dispositivo móvil;

- Dominio de código n/1 (DCn/1) incluyendo funciones ($f1_{DCn/1}$, $f2_{DCn/1,}$ …) de la aplicación software de dispositivo móvil;

- Dominio de código n/2 (DCn/2) incluyendo funciones ($f1_{DCn/2}$, $f2_{DCn/2,}$ …) de la aplicación software de dispositivo móvil;

Conforme a algunas implementaciones:

- Instrucciones de código de ($f1_{DC2/1}$, $f2_{DC2/1,}$ …) en DC2/1 de la aplicación son respectivamente equivalentes en términos de funcionalidad que instrucciones de código de ($f1_{DC3/1}$, $f2_{DC3/1,}$ …) en DC3/1 de la aplicación;

- e instrucciones de código de ($f1_{DC2/1}$, $f2_{DC2/1,}$ …) en DC2/1 de la aplicación, e instrucciones de código de ($f1_{DC3/1}$, $f2_{DC3/1,}$ …) en DC3/1 de la aplicación, son cada una respectivamente equivalentes en términos de funcionalidad que instrucciones de código de ($f1_{DC4/1}$, $f2_{DC4/1,}$ …) en DC4/1 de la aplicación;

- e instrucciones de código de ($f1_{DC2/1}$, $f2_{DC2/1,}$ …) en DC2/1 de la aplicación, e instrucciones de código de ($f1_{DC3/1}$, $f2_{DC3/1,}$ …) en DC3/1 de la aplicación, …, e instrucciones de código de ($f1_{DCn-1/1}$, $f2_{DCn-1/1,}$ …) en DCn-1/1 de la aplicación, son cada una respectivamente equivalentes en términos de funcionalidad que instrucciones de código de ($f1_{DCn/1}$, $f2_{DCn/1,}$ …) en DCn/1 de la aplicación;

- e instrucciones de código de ($f1_{DC2/2}$, $f2_{DC2/2,}$ …) en DC2/2 de la aplicación son respectivamente equivalentes en términos de funcionalidad que instrucciones de código de ($f1_{DC3/2}$, $f2_{DC3/2,}$ …) en DC3/2 de la aplicación;

- e instrucciones de código de ($f1_{DC2/2}$, $f2_{DC2/2,}$ …) en DC2/2 de la aplicación, e instrucciones de código de ($f1_{DC3/2}$, $f2_{DC3/2,}$ …) en DC3/2 de la aplicación, son cada una respectivamente equivalentes en términos de funcionalidad que instrucciones de código de ($f1_{DC4/2}$, $f2_{DC4/2,}$ …) en DC4/2 de la aplicación;

- e instrucciones de código de ($f1_{DC2/2}$, $f2_{DC2/2,}$ …) en DC2/2 de la aplicación, e instrucciones de código de ($f1_{DC3/2}$, $f2_{DC3/2,}$ …) en DC3/2 de la aplicación, …, e instrucciones de código de ($f1_{DCn-1/2}$, $f2_{DCn-1/2,}$ …) en DCn-1/2 de la aplicación, son cada una respectivamente equivalentes en términos de funcionalidad que instrucciones de código de ($f1_{DCn/2}$, $f2_{DCn/2,}$ …) en DCn/2 de la aplicación.

Por tanto, ventajosamente, en esas implementaciones la aplicación software de dispositivo móvil puede conseguir el mismo nivel de funcionalidad usando [($f1_{DCk/1}$, $f2_{DCk/1,}$ …) en DCk/1 y ($f1_{DCk/2}$, $f2_{DCk/2,}$ …) en DCk/2] que usando [($f1_{DCl/1}$, $f2_{DCl/1,}$ …) en DCl/1 y ($f1_{DCl/2}$, $f2_{DCl/2,}$ …) en DCl/2], k y l en el rango de 2 a n.

Como ya se ha mencionado en relación a la figura 1, paso (2), el proveedor de servicios de personalización usa una aplicación software de dispositivo móvil, un registro de personalización de seguridad (ej. RPS-I) y software de protección de seguridad que están almacenados en una o más memorias para generar usando uno o más dispositivos de procesamiento una aplicación software protegida de dispositivo móvil que es personalizada en términos de seguridad usando datos del registro de personalización de seguridad.

La figura 2.b ilustra la protección de seguridad aplicada por el software de protección de seguridad a la aplicación software de dispositivo móvil en una implementación particular. El proceso de protección utiliza el registro de personalización de seguridad de inicialización (RPS-I) descrito en la figura 2.a para generar la aplicación software protegida de dispositivo móvil personalizada en seguridad.

En esta implementación los sub registros de seguridad genérica (RS_1, RS_2, RS_3, RS_4, …, RS_i, …, RS_n) y los sub registros de personalización de seguridad (RPS_{21}, RPS_{31}, RPS_{41}, …, RPS_{i1}, …, RPS_{n1}) del RPS-I incluyen parámetros de seguridad (ps), reglas de ofuscación (ro) y redes de checksums (ch), como los ilustrados en la figura 2.a. En esta implementación al menos parte de los checksums de las redes de checksums del registro de

personalización de seguridad son calculados como checksums del código de la aplicación y de parámetros de seguridad del registro de personalización de seguridad.

En esta implementación un proceso de ofuscación es aplicado por el software de protección de seguridad al código de la aplicación software de dispositivo móvil, y a parámetros de seguridad del registro de personalización de seguridad que están al menos parcialmente embebidos en el código de la aplicación y/o que están al menos parcialmente almacenados en la base de datos de la aplicación por el software de protección de seguridad, y a checksums de las redes de checksums del registro de personalización de seguridad que están al menos parcialmente embebidos en el código de la aplicación y/o que están al menos parcialmente almacenados en la base de datos de la aplicación por el software de protección de seguridad. Los detalles son los siguientes:

- datos de RS1 son embebidos en el código de la aplicación de las funciones DC1($f1_{DC1}$, $f2_{DC1,}$ …), y dicho código de la aplicación de las funciones DC1($f1_{DC1}$, $f2_{DC1,}$ …), junto con los parámetros de seguridad [$ps_{1\text{-}RS1}$, …, $ps_{r\text{-}RS1}$] embebidos de RS1 y las redes de checksums [$ch_{1\text{-}RS1}$, …, $ch_{r\text{-}RS1}$] embebidas de RS1, son ofuscados usando al menos parte de las reglas de ofuscación [$ro_{1\text{-}RS1}$, …, $ro_{r\text{-}RS1}$] embebidas. Por tanto, las funciones de DC1 quedan protegidas a través de la ofuscación del código de las funciones de DC1 y los parámetros de seguridad y redes de checksums de RS1 embebidos, usando las reglas de ofuscación embebidas (ej. parte de ellas podrían estar protegidas mediante otras reglas de ofuscación). Dicha protección es ilustrada en la figura 2.b como $P1_{RS1}$ (protección de DC1 usando RS1).

- Datos de RS2 son embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …), y dicho código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …), junto con los parámetros de seguridad [$ps_{1a\text{-}RS2}$, …, $ps_{m\text{-}RS2}$] embebidos de RS2 y las redes de checksums [$ch_{1a\text{-}RS2}$, …, $ch_{m\text{-}RS2}$] embebidas de RS2, son ofuscados usando reglas de ofuscación ($ro_{1a\text{-}RS2}$, …, $ro_{m\text{-}RS2}$) que son al menos parcialmente embebidas en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) y que pueden también ser al menos parcialmente almacenadas en la parte correspondiente de la base de datos de la aplicación (ej. parte de $ro_{1b\text{-}RPS21}$ y $ro_{2b\text{-}rps21}$). Por tanto las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) quedan protegidas a través de la ofuscación del código de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y DC2/2($f1_{DC2/2}$, $f2_{CD2/2,}$ …) y los parámetros de seguridad y redes de checksums de RS2 embebidos, usando reglas de ofuscación que son al menos parcialmente embebidas en las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) y que pueden ser al menos parcialmente almacenadas en la base de datos de la aplicación. Dicha protección es ilustrada en la figura 2.b como $P2_{RS2}$ (protección de DC2/1 y DC2/2 basada en datos RS2 embebidos).

- Datos de RPS21 son almacenados en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a DC2/1 and DC2/2 tal que el código de la aplicación de las funciones de DC2/1 y DC2/2 queda también protegido mediante los parámetros de seguridad, reglas de ofuscación y redes de checksums de RPS21. Dicha protección es ilustrada en la figura 2.b como $P2_{RPS21}$ (protección de DC2/1 y DC2/2 basada en datos almacenados de RPS21).

  - [$ps_{1a\text{-}RS2}$] y [$ps_{1b\text{-}RPS21}$] son las dos partes del mismo parámetro de seguridad, y en esta implementación [$ps_{1a\text{-}RS2}$] es embebido en DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …).

  - [$ro_{1a\text{-}RS2}$] y [$ro_{1b\text{-}RPS21}$] son las dos partes de la misma regla de ofuscación, y en esta implementación [$ro_{1a\text{-}RS2}$] es embebida en DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …).

  - [$ch_{1a\text{-}RS2}$] y [$ch_{1b\text{-}RPS21}$] son las dos partes de la misma red de checksums, y en esta implementación [$ch_{1a\text{-}RS2}$] es embebido en DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …).

  - [$ps_{2a\text{-}RS2}$] y [$ps_{2b\text{-}RPS21}$] son las dos partes del mismo parámetro de seguridad, y en esta implementación [$ps_{2a\text{-}RS2}$] es embebido en DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …).

  - [$ro_{2a\text{-}RS2}$] y [$ro_{2b\text{-}RPS21}$] son las dos partes de la misma regla de ofuscación, y en esta implementación [$ro_{2a\text{-}RS2}$] es embebida en DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …).

  - [$ch_{2a\text{-}RS2}$] y [$ch_{2b\text{-}RPS21}$] son las dos partes de la misma red de checksums, y en esta implementación [$ch_{2a\text{-}RS2}$] es embebido en DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …).

- datos de RSn son embebidos en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …), y dicho código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y

DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …), junto con los parámetros de seguridad [$ps_{1a\text{-}RSn}$, …, $ps_{t\text{-}RSn}$] embebidos de RSn y las redes de checksums [$ch_{1a\text{-}RSn}$, …, $ch_{t\text{-}RSn}$] embebidas de RSn, son ofuscados usando reglas de ofuscación ($ro_{1a\text{-}RSn}$, …, $ro_{t\text{-}RSn}$) que son al menos parcialmente embebidas en el código de aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) y que pueden también ser al menos parcialmente almacenadas en la parte correspondiente de la base de datos de la aplicación (ej. parte de $ro_{1b\text{-}RPSn1}$ y $ro_{2b\text{-}RPSn1}$). Por tanto las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y DCn/2($f1_{CDn/2}$, $f2_{DCn/2,}$ …) quedan protegidas a través de la ofuscación del código de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) y los parámetros de seguridad y redes de checksums de RSn embebidos, usando reglas de ofuscación que son al menos parcialmente embebidas en las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) y que pueden ser al menos parcialmente almacenadas en la base de datos de la aplicación. Dicha protección es ilustrada en la figura 2.b como Pn_{RSn} (protección de DCn/1 y DCn/2 basada en datos RSn embebidos).

- Datos de RPSn1 son almacenados en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a DCn/1 and DCn/2 tal que el código de la aplicación de las funciones de DCn/1 y DCn/2 queda también protegido mediante los parámetros de seguridad, reglas de ofuscación y redes de checksums de RPSn1. Dicha protección es ilustrada en la figura 2.b como Pn_{RPSn1} (protección de DCn/1 y DCn/2 basada en datos almacenados de RPSn1).

  - [$ps_{1a\text{-}RSn}$] y [$ps_{1b\text{-}RPSn1}$] son las dos partes del mismo parámetro de seguridad, y en esta implementación [$ps_{1a\text{-}RSn}$] es embebido en DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …).

  - [$ro_{1a\text{-}RSn}$] and [$ro_{1b\text{-}RPSn1}$] son las dos partes de la misma regla de ofuscación, y en esta implementación [$ro_{1a\text{-}RSn}$] es embebida en DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …).

  - [$ch_{1a\text{-}RSn}$] and [$ch_{1b\text{-}RPSn1}$] son las dos partes de la misma red de checksums, y en esta implementación [$ch_{1a\text{-}RSn}$] es embebido en DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …).

  - [$ps_{2a\text{-}RSn}$] and [$ps_{2b\text{-}RPSn1}$] son las dos partes del mismo parámetro de seguridad, y en esta implementación [$ps_{2a\text{-}RSn}$] es embebido en DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …).

  - [$ro_{2a\text{-}RSn}$] and [$ro_{2b\text{-}RPSn1}$] son las dos partes de la misma regla de ofuscación, y en esta implementación [$ro_{2a\text{-}RSn}$] es embebida en DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …).

  - [$ch_{2a\text{-}RSn}$] and [$ch_{2b\text{-}RPSn1}$] son las dos partes de la misma red de checksums, y en esta implementación [$ch_{2a\text{-}RSn}$] es embebido en DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …).

Cuando instrucciones de código de una función o conjunto de funciones dadas de la aplicación software protegida de dispositivo móvil son ejecutadas por uno o más procesadores del dispositivo móvil, una operación regular de dicha función o conjunto de funciones puede requerir usar ciertos parámetros de seguridad, reglas de ofuscación y/o redes de checksums. Conforme a algunas implementaciones, al menos partes de esos parámetros de seguridad, reglas de ofuscación y/o redes de cheksums son para ser almacenados (/y ofuscados) en la base de datos de la aplicación, y si dichas partes no están disponibles en la correspondiente parte de la base de datos de la aplicación, o los valores no son correctos, entonces dicha función o conjunto de funciones no están habilitadas para operación regular, y el dominio(s) de código que incluye dicha función o conjunto de funciones esta (/están) también no habilitado para operación regular en relación a dicha función o conjunto de funciones.

Un intento de ejecutar instrucciones de código de una de esas funciones sin que los datos adecuados estén disponibles en la correspondiente parte de la base de datos de la aplicación puede causar una reacción de protección definida/esperada de la aplicación software protegida de dispositivo móvil (ej. la aplicación detiene su ejecución), puede causar un rechazo posterior por el proveedor de servicios de una solicitud de servicio recibida desde la aplicación software protegida de dispositivo móvil, etc., como consecuencia de la una o más funciones no estando habilitadas para operación regular.

La figura 2.c es relativa a algunas implementaciones de aplicar una protección de seguridad a funciones en DC2/1, DC2/2, DC3/1, DC3/2, …, DCn/1 y DCn/2, en el contexto de generar una aplicación software protegida de dispositivo móvil como la referida en la figura 2.b

En esta implementación, en términos de parámetros de seguridad de RS2 y RPS21:

- [$ps_{1a\text{-}RS2}$, $ps_{3\text{-}RS2,}$ $ps_{4\text{-}RS2}$ …, $ps_{g\text{-}RS2}$] son embebidos (hard-coded) en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …).

- [$ps_{1a\text{-}RS2}$] y [$ps_{1b\text{-}RPS21}$] son las dos partes del mismo parámetro de seguridad. La figura 2.c ilustra que [$ps_{1a\text{-}RS2}$] es embebido en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …) y [$ps_{1b\text{-}RPS21}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DC2/1. La figura 2.c también se refiere a la posibilidad de que [$ps_{1b\text{-}RPS21}$] sea almacenado en formato ofuscado como se describe en la figura 2.d.

- [$ps_{2a\text{-}RS2}$, $ps_{(g+1)\text{-}RS2,}$ $ps_{(g+2)\text{-}RS2}$ …, $ps_{m\text{-}RS2}$] son embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2,}$ $f2_{DC2/2,}$ …).

- [$ps_{2a\text{-}RS2}$] y [$ps_{2b\text{-}RPS21}$] son las dos partes del mismo parámetro de seguridad. La figura 2.c ilustra que [$ps_{2a\text{-}RS2}$] es embebido en el código de la aplicación de las funciones DC2/2($f1_{DC2/2,}$ $f2_{DC2/2,}$ …) y [$ps_{2b\text{-}RPS21}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DC2/2. La figura 2.c también se refiere a la posibilidad de que [$ps_{2b\text{-}RPS21}$] sea almacenado en formato ofuscado como se describe en la figura 2.d.

En términos de las redes de checksums de RS2 and RPS21:

- [$ch_{1a\text{-}RS2}$, $ch_{3\text{-}RS2,}$ $ch_{4\text{-}RS2}$ …, $ch_{g\text{-}RS2}$] y [$ch_{1b\text{-}RPS21}$] son calculados como checksums de partes del código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …) y de al menos partes de uno o más parámetros de seguridad [$ps_{1a\text{-}RS2}$, $ps_{3\text{-}RS2,}$ $ps_{4\text{-}RS2}$ …, $ps_{g\text{-}RS2}$] embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …).

- [$ch_{1a\text{-}RS2}$, $ch_{3\text{-}RS2,}$ $ch_{4\text{-}RS2}$ …, $ch_{g\text{-}RS2}$] son embebidos (hard-coded) en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …).

- [$ch_{1a\text{-}RS2}$] y [$ch_{1b\text{-}RPS21}$] son las dos partes de la misma red de checksums. La figura 2.c ilustra que [$ch_{1a\text{-}RS2}$] está embebido en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …) y [$ch_{1b\text{-}RPS21}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DC2/1. La figura 2.c también se refiere a la posibilidad de que [$ch_{1b\text{-}RPS21}$] sea almacenado en formato ofuscado como se describe en la figura 2.d.

- [$ch_{2a\text{-}RS2}$, $ch_{(g+1)\text{-}RS2,}$ $ch_{(g+2)\text{-}RS2}$ …, $ch_{m\text{-}RS2}$] y [$ch_{2b\text{-}RPS21}$] son calculados como checksums de partes del código de la aplicación de las funciones DC2/2($f1_{DC2/2,}$ $f2_{DC2/2,}$ …) y de al menos partes de uno más parámetros de seguridad [$ps_{2a\text{-}RS2}$, $ps_{(g+1)\text{-}RS2,}$ $ps_{(g+2)\text{-}RS2}$ …, $ps_{m\text{-}SR2}$] embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2,}$ $f2_{DC2/2,}$ …).

- [$ch_{2a\text{-}RS2}$, $ch_{(g+1)\text{-}RS2,}$ $ch_{(g+2)\text{-}RS2}$ …, $ch_{m\text{-}RS2}$] son embebidos (hard-coded) en el código de la aplicación de las funciones DC2/2($f1_{DC2/2,}$ $f2_{DC2/2,}$ …).

- [$ch_{2a\text{-}RS2}$] y [$ch_{2b\text{-}RPS21}$] son las dos partes de la misma red de checksums. La figura 2.c ilustra que [$ch_{2a\text{-}RS2}$] está embebido en el código de la aplicación de las funciones DC2/2($f1_{DC2/2,}$ $f2_{DC2/2,}$ …) y [$ch_{2b\text{-}RPS21}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DC2/2. La figura 2.c también se refiere a la posibilidad de que [$ch_{2b\text{-}RPS21}$] sea almacenado en formato ofuscado como se describe en la figura 2.d.

En términos de reglas de ofuscación de RS2 and RPS21:

- [$ro_{1a\text{-}RS2}$, $ro_{3\text{-}RS2,}$ $ro_{4\text{-}RS2}$ …, $ro_{g\text{-}RS2}$] son embebidas en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …).

- El código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …) junto con los [$ps_{1a\text{-}RS2}$, $ps_{3\text{-}RS2,}$ $ps_{4\text{-}RS2}$ …, $ps_{g\text{-}RS2}$] y [$ch_{1a\text{-}RS2}$, $ch_{3\text{-}RS2,}$ $ch_{4\text{-}RS2}$ …, $ch_{g\text{-}RS2}$] embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …) son ofuscados usando [$ro_{1a\text{-}RS2}$, $ro_{3\text{-}RS2,}$ $ro_{4\text{-}RS2}$ …, $ro_{g\text{-}RS2}$] y [$ro_{1b\text{-}RPS21}$].

- [$ro_{1a\text{-}RS2}$] y [$ro_{1b\text{-}RPS21}$] son las dos partes de la misma regla de ofuscación. La figura 2.c illustra que [$ro_{1a\text{-}RS2}$] está embebida en el código de la aplicación de las funciones DC2/1($f1_{DC2/1,}$ $f2_{DC2/1,}$ …) y [$ro_{1b\text{-}RPS21}$] es almacenada en una parte de la base de datos de la aplicación que está asociada a DC2/1. La figura 2.c también se refiere a la posibilidad de que [$ro_{1b\text{-}RPS21}$] sea almacenada en formato ofuscado como se describe en la figura 2.d.

- [$ro_{2a\text{-}RS2}$, $ro_{(g+1)\text{-}RS2,}$ $ro_{(g+2)\text{-}RS2}$ …, $ro_{m\text{-}RS2}$] son embebidas en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …).

- El código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) junto con los [$ps_{2a\text{-}RS2}$, $ps_{(g+1)\text{-}RS2,}$ $ps_{(g+2)\text{-}RS2}$ …, $ps_{m\text{-}RS2}$] y [$ch_{2a\text{-}RS2}$, $ch_{(g+1)\text{-}RS2,}$ $ch_{(g+2)\text{-}RS2}$ …, $ch_{m\text{-}RS2}$] embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) son ofuscados usando [$ro_{2a\text{-}RS2}$, $ro_{(g+1)\text{-}RS2,}$ $ro_{(g+2)\text{-}RS2}$ …, $ro_{m\text{-}RS2}$] y [$ro_{2b\text{-}RPS21}$].

- [$ro_{2a\text{-}RS2}$] y [$ro_{2b\text{-}RPS21}$] son las dos partes de la misma regla de ofuscación. La Figura 2.c illustra que [$ro_{2a\text{-}RS2}$] es embebida en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) y [$ro_{2b\text{-}RPS21}$] es almacenada en una parte de la base de datos de la aplicación que está asociada a DC2/2. La figura 2.c también se refiere a la posibilidad de que [$ro_{2b\text{-}RPS21}$] sea almacenada en formato ofuscado como se describe en la figura 2.d.

En términos de parámetros de seguridad de RSi y RPSi1:

En términos de redes de checksums de RSi y RPSi1:

En términos de reglas de ofuscación de RSi y RPSi1:

En esta implementación, en términos de parámetros de seguridad de RSn and RPSn1:

- [$ps_{1a\text{-}RSn}$, $ps_{3\text{-}RSn,}$ $ps_{4\text{-}RSn}$ …, $ps_{j\text{-}RSn}$] son embebidos (hard-coded) en el código de la aplicación de las funciones CDn/1($f1_{CDn/1}$, $f2_{CDn/1,}$ …).

- [$ps_{1a\text{-}RSn}$] y [$ps_{1b\text{-}RPSn1}$] son las dos partes del mismo parámetro de seguridad. [$ps_{1a\text{-}RSn}$] es embebido en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y [$ps_{1b\text{-}RPSn1}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DCn/1.

- [$ps_{2a\text{-}RSn}$, $ps_{(j+1)\text{-}RSn,}$ $ps_{(j+2)\text{-}RSn}$ …, $ps_{t\text{-}RSn}$] son embebidos en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …).

- [$ps_{2a\text{-}RSn}$] y [$ps_{2b\text{-}RPSn1}$] son las dos partes del mismo parámetro de seguridad. [$ps_{2a\text{-}RSn}$] es embebido en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) y [$ps_{2b\text{-}RPSn1}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DCn/2.

En términos de las redes de checksums de RSn y RPSn1:

- [$ch_{1a\text{-}RSn}$, $ch_{3\text{-}RSn,}$ $ch_{4\text{-}RSn}$ …, $ch_{j\text{-}RSn}$] y [$ch_{1b\text{-}RPSn1}$] son calculados como checksums de partes del código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y de al menos partes de uno o más parámetros de seguridad [$ps_{1a\text{-}RSn}$, $ps_{3\text{-}RSn,}$ $ps_{4\text{-}RSn}$ …, $ps_{j\text{-}RSn}$] embebidos en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …).

- [$ch_{1a\text{-}RSn}$, $ch_{3\text{-}RSn,}$ $ch_{4\text{-}RSn}$ …, $ch_{j\text{-}RSn}$] son embebidos (hard-coded) en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …).

- [$ch_{1a\text{-}RSn}$] y [$ch_{1b\text{-}RPSn1}$] son las dos partes de la misma red de checksums. [$ch_{1a\text{-}RSn}$] es embebido en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y [$ch_{1b\text{-}RPSn1}$] es almacenado en un parte de la base de datos de la aplicación que está asociada a DCn/1.

- [$ch_{2a\text{-}RSn}$, $ch_{(j+1)\text{-}RSn,}$ $ch_{(j+2)\text{-}RSn}$ …, $ch_{t\text{-}RSn}$] y [$ch_{2b\text{-}RPSn1}$] son calculados como checksums de partes del código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) y de al menos partes de uno o más parámetros de seguridad [$ps_{2a\text{-}RSn}$, $ps_{(j+1)\text{-}RSn,}$ $ps_{(j+2)\text{-}RSn}$ …, $ps_{t\text{-}RSn}$] embebidos en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …).

- [$ch_{2a\text{-}RSn}$, $ch_{(j+1)\text{-}RSn,}$ $ch_{(j+2)\text{-}RSn}$ …, $ch_{t\text{-}RSn}$] son embebidos (hard-coded) en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …).

- [$ch_{2a\text{-}RSn}$] y [$ch_{2b\text{-}RPSn1}$] son las dos partes de la misma red de checksums. [$ch_{2a\text{-}RSn}$] es embebido en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) y [$ch_{2b\text{-}RPSn1}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DCn/2.

En términos de reglas de ofuscación de RSn y RPSn1:

- [$ro_{1a\text{-}RSn}$, $ro_{3\text{-}RSn}$, $ro_{4\text{-}RSn}$ …, $ro_{j\text{-}RSn}$] son embebidas en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …).

- El código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) junto con los [$ps_{1a\text{-}RSn}$, $ps_{3\text{-}RSn,}$ $sp_{4\text{-}RSn}$ …, $ps_{j\text{-}RSn}$] y [$ch_{1a\text{-}RSn}$, $ch_{3\text{-}RSn,}$ $ch_{4\text{-}RSn}$ …, $ch_{j\text{-}RSn}$] embebidos en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) son ofuscados usando [$ro_{1a\text{-}RSn}$, $ro_{3\text{-}RSn,}$ $ro_{4\text{-}RSn}$ …, $ro_{j\text{-}RSn}$] y [$ro_{1b\text{-}RPSn1}$].

- [$ro_{1a\text{-}RSn}$] y [$ro_{1b\text{-}RPSn1}$] son las dos partes de la misma regla de ofuscación. [$ro_{1a\text{-}RSn}$] es embebida en el código de la aplicación de las funciones DCn/1($f1_{DCn/1}$, $f2_{DCn/1,}$ …) y [$ro_{1b\text{-}RPSn1}$] es almacenada en una parte de la base de datos de la aplicación que está asociada a DCn/1.

- [$ro_{2a\text{-}RSn}$, $ro_{(j+1)\text{-}RSn,}$ $ro_{(j+2)\text{-}RSn}$ …, $ro_{t\text{-}RSn}$] son embebidas en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …).

- El código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) junto con los [$ps_{2a\text{-}RSn}$, $ps_{(j+1)\text{-}RSn,}$ $ps_{(j+2)\text{-}RSn}$ …, $ps_{t\text{-}RSn}$] y [$ch_{2a\text{-}RSn}$, $ch_{(j+1)\text{-}RSn,}$ $ch_{(j+2)\text{-}RSn}$ …, $ch_{t\text{-}RSn}$] embebidos en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) son ofuscados usando [$ro_{2a\text{-}RSn}$, $ro_{(j+1)\text{-}RSn,}$ $ro_{(j+2)\text{-}RSn}$ …, $ro_{t\text{-}RSn}$] y [$ro_{2b\text{-}RPSn1}$].

- [$ro_{2a\text{-}RSn}$] y [$ro_{2b\text{-}RPSn1}$] son las dos partes de la misma regla de ofuscación. [$ro_{2a\text{-}RSn}$] está embebida en el código de la aplicación de las funciones DCn/2($f1_{DCn/2}$, $f2_{DCn/2,}$ …) y [$ro_{2b\text{-}RPSn1}$] está almacenada en una parte de la base de datos de la aplicación que está asociada a DCn/2.

La figura 2.d es relativa a algunas implementaciones asociadas a la ofuscación de al menos partes de parámetros de seguridad, reglas de ofuscación y datos de redes de checksums en una parte de la base de datos de la aplicación que está asociada a un dominio de código dado, en el contexto de generar una aplicación software protegida de dispositivo móvil como la referida en las figuras 2.b y 2.c.

Como se describe en la figura 2.c, en relación a RSx y RPSx1 (x = 2, 3, 4,…, i, …, n)

- [$ps_{1a\text{-}RSx}$] y [$ps_{1b\text{-}RPSx1}$] son las dos partes del mismo parámetro de seguridad y [$ps_{1b\text{-}RPSx1}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DCx/1.

- [$ch_{1a\text{-}RSx}$] y [$ch_{1b\text{-}RPSx1}$] son las dos partes de la misma red de checksums y [$ch_{1b\text{-}RPSx1}$] es almacenada en una parte de la base de datos de la aplicación que está asociada a DCx/1.

- [$ro_{1a\text{-}RSx}$] y [$ro_{1b\text{-}RPSx1}$] son las dos partes de la misma regla de ofuscación y [$ro_{1b\text{-}RPSx1}$] es almacenada en una parte de la base de datos de la aplicación que está asociada a DCx/1.

Conforme a algunas implementaciones [$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] son ofuscados por el software de protección de seguridad antes de ser almacenados en la parte correspondiente de la base de datos de la aplicación asociada a DCx/1 (la figura 2.d ilustra el almacenamiento en la parte DCx/1 – RPSx1 de la base de datos de la aplicación).

La figura 2.d muestra un proceso de ofuscar [$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] utilizando un algoritmo de ofuscación (ej. un algoritmo BPS de reservación del formato de datos) y una clave, para proteger esos datos de personalización de seguridad DCx/1. En particular, la figura 2.d ilustra una clave de ofuscación constituida por un checksum x/1 de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad que está hard-coded (embebido) en el dominio de código DC1 (en relación a DCx/1) como parte de $P1_{RS1}$, y al menos una parte de un identificador del dispositivo (ej. una parte del MSISDN; para propósito de test por el proveedor de servicios de personalización, un identificador de dispositivo de test – IDD_{TEST} – puede ser usado como parte de la clave de ofuscación, como se ilustra en la figura 2.d).

En estas implementaciones DCx/1 son primeros dominios de código y DC1 es un segundo dominio de código, y DCx/1 está vinculado e términos de seguridad a DC1 mediante la personalización de [$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] en formato ofuscado en la parte correspondiente de la base de datos de la aplicación.

En la implementación ilustrada en la figura 2.d, cada vinculación DCx/1 – DC1 depende de un parámetro de seguridad que está hard-coded (embebido) en el código de la aplicación de DC1 (en relación a DCx/1). Dicho

parámetro de seguridad es requerido por el código de la aplicación de DCx/1 para des ofuscar adecuadamente [$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] para uso, según definido, por el código de la aplicación de DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …). Por tanto, un parámetro de seguridad disponible en DC1 es requerido para habilitar DCx/1 para operación regular.

En un ejemplo particular, el parámetro de seguridad de DC1 ha sido ofuscado usando una regla de ofuscación embebida en el código de la aplicación de DC1, por tanto la regla de ofuscación disponible en DC1 (en relación al parámetro de seguridad) es requerida para habilitar DCx/1 para operación regular (es decir, es requerida para des ofuscar el parámetro de seguridad, que es requerido como parte de la clave para des ofuscar [$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$], por lo que la regla de ofuscación es requerida para habilitar DCx/1 para operación regular).

En un ejemplo particular, el parámetro de seguridad ha sido usado para calcular una red de checksums que está embebida en el código de la aplicación de DC1, por lo que una adecuada verificación de la red de checksums por el código de aplicación de DC1 es requerida, para habilitar DCx/1 para operación regular (ej. si la red de checksums no es adecuadamente verificada, el código de aplicación de DC1 detendrá su ejecución, por lo que el parámetro de seguridad de CD1 no podrá ser obtenido, y DCx/1 no será habilitado para operación regular).

Ventajosamente, la aplicación generada incluye varios dominios de código, relativos a los uno o más proveedores de servicio, donde uno o más primeros dominios de código (ej. DCx/1) son vinculados en términos de seguridad a uno o más segundos dominios de código (ej. DC1) a través de la personalización de seguridad ([$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] and [$ro_{1b\text{-}RPSx1}$] almacenados en la base de datos de la aplicación en formato ofuscado), dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código (el parámetro de seguridad y/o regla de ofuscación y/o datos checksums en DC1 referidos anteriormente) y que son requeridos para habilitar los uno o más primeros dominios de código para operación regular (ej. que es/son requeridos para des ofuscar ([$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] para uso por DCx/1).

Conforme a algunas implementaciones cada uno de [$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] es ofuscado usando una clave de ofuscación diferente. En un ejemplo particular:

- La clave usada para ofuscar [$ps_{1b\text{-}RPSx1}$] está constituida por un checksum de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad (ej. [$ps_{ix\text{-}RS1}$]) que está hard-coded (embebido) en el código de la aplicación de DC1 (en relación a DCx/1) como parte de $P1_{RS1}$, y una parte de un identificador de dispositivo (ej. el MSISDN o un cálculo basado en el MSISDN, la dirección MAC, etc.).

- La clave usada para ofuscar [$ch_{1b\text{-}RPSx1}$] está constituida por un checksum de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad (ej. [$ps_{jx\text{-}RS1}$]) que está hard-coded (embebido) en el código de la aplicación de DC1 (en relación a DCx/1) como parte de $P1_{RS1}$, y una parte de un identificador de dispositivo.

- La clave usada para ofuscar [$ro_{1b\text{-}RPSx1}$] está constituida por un checksum de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad (ej. [$ps_{kx\text{-}RS1}$]) que está hard-coded (embebido) en el código de la aplicación de DC1 (en relación a DCx/1) como parte de $P1_{RS1}$, y una parte de un identificador de dispositivo.

Para propósitos de test por el proveedor de servicios de personalización, un identificador de dispositivo de test – IDD_{TEST} – puede ser usado como parte de la correspondiente clave de ofuscación.

En estas implementaciones, DCx/1 (primeros dominios de código) son también vinculados en términos de seguridad a DC1 (segundo dominio de código) mediante la personalización de [$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] and [$ro_{1b\text{-}RPSx1}$] en formato ofuscado en la parte correspondiente de la base de datos de la aplicación.

Cada vinculación DCx/1 – DC1 depende, respectivamente en términos de [$ps_{1b\text{-}RPSx1}$] / [$ch_{1b\text{-}RPSx1}$] / [$ro_{1b\text{-}RPSx1}$], del parámetro de seguridad [$ps_{ix\text{-}RS1}$] / [$ps_{jx\text{-}RS1}$] / [$ps_{kx\text{-}RS1}$]. Dicho parámetro de seguridad [$ps_{ix\text{-}RS1}$] / [$ps_{jx\text{-}RS1}$] / [$ps_{kx\text{-}RS1}$] es requerido por el código de la aplicación de DCx/1 para respectivamente y adecuadamente des ofuscar [$ps_{1b\text{-}RPSx1}$] / [$ch_{1b\text{-}RPSx1}$] / [$ro_{1b\text{-}RPSx1}$] para uso, según definido, por el código de la aplicación de DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …). Por tanto, parámetros de seguridad disponibles en DC1 son requeridos para habilitar DCx/1 para operación regular.

En un ejemplo particular, los parámetros de seguridad [$ps_{ix\text{-}RS1}$] / [$ps_{jx\text{-}SR1}$] / [$ps_{kx\text{-}RS1}$] de DC1 han sido ofuscados usando una o más reglas de ofuscación embebidas en el código de la aplicación de DC1, por lo que reglas de ofuscación disponibles en DC1 (en relación a los parámetros de seguridad) son requeridas para habilitar DCx/1 para operación regular (es decir son requeridas para des ofuscar los parámetros de seguridad, que son requeridos para calcular las claves de des ofuscación, por lo que las reglas de ofuscación son requeridas para habilitar DCx/1 para operación regular).

En un ejemplo particular, los parámetros de seguridad [$ps_{ix\text{-}RS1}$] / [$ps_{jx\text{-}RS1}$] / [$ps_{kx\text{-}RS1}$] han sido usados para calcular una o más redes de checksums que están embebidas en el código de la aplicación de DC1, por lo que una verificación adecuada de las redes de checksums por el código de la aplicación de DC1 es requerida para habilitar DCx/1 para operación regular (ej. si las redes de checksums no son adecuadamente verificadas, el código de la aplicación de DC1 detendrá su ejecución, por lo que los parámetros de seguridad de DC1 no serán obtenidos, y DCx/1 no será habilitado para operación regular).

Ventajosamente, la aplicación generada incluye varios dominios de código, relativos a los uno o más proveedores de servicios, donde uno o más primeros dominios de código (ej. DCx/1) son vinculados en términos de seguridad a uno o más segundos dominios de código (ej. DC1) a través de la personalización de seguridad ([$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] almacenados en la base de datos de la aplicación en formato ofuscado), dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código (el parámetro de seguridad y/o regla de ofuscación y/o datos de checksums en DC1 referidos anteriormente) y que son requeridos para habilitar los uno o más primeros dominios de código para operación regular (ej. que es/son requeridos para des ofuscar ([$ps_{1b\text{-}RPSx1}$], [$ch_{1b\text{-}RPSx1}$] y [$ro_{1b\text{-}RPSx1}$] para uso por DCx/1).

Como también se describe en la figura 2.c, en relación a RSx y RPSx1 (x = 2, 3, 4,…, i, …, n)

- [$ps_{2a\text{-}RSx}$] y [$ps_{2b\text{-}RPSx1}$] son las dos partes del mismo parámetro de seguridad y [$ps_{2b\text{-}RPSx1}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DCx/2.

- [$ch_{2a\text{-}RSx}$] y [$ch_{2b\text{-}RPSx1}$] son las dos partes de la misma red de checksums y [$ch_{2b\text{-}RPSx1}$] es almacenado en una parte de la base de datos de la aplicación que está asociada a DCx/2.

- [$ro_{2a\text{-}RSx}$] y [$ro_{2b\text{-}RPSx1}$] son las dos partes de la misma regla de ofuscación y [$ro_{2b\text{-}RPSx1}$] es almacenada en una parte de la base de datos de la aplicación que está asociada a DCx/2.

Conforme a algunas implementaciones [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] son ofuscados por el software de protección de seguridad antes de ser almacenados en la parte correspondiente de la base de datos de la aplicación asociada a DCx/2 (la figura 2.d ilustra el almacenamiento en la parte DCx/2 – RPSx1 de la base de datos de la aplicación).

La figura 2.d muestra un proceso de ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] usando un algoritmo de ofuscación y una clave, para proteger esos datos de personalización de seguridad DCx/2. En particular, la figura 2.d ilustra una clave de ofuscación constituida por un checksum x/2 de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad que está al menos parcialmente hard-coded (embebido) en el dominio de código DCx/1 (en relación a DCx/2) como parte de Px_{RSx}, y al menos una parte de un identificador de dispositivo (ej. al menos una parte del MSISDN; para propósitos de test por el proveedor de servicios de personalización, un identificador de dispositivo de test – IDD_{TEST} – puede ser usado como parte de la clave de ofuscación, como se ilustra en la figura 2.d).

Conforme a algunas implementaciones el parámetro de seguridad está al menos parcialmente hard-coded en el domino de código DCx/1 y parcialmente almacenado en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a DCx/1. En un ejemplo particular, la parte hard-coded en el domino de código DCx/1 (en relación a DCx/2) es al menos una parte de [$ps_{1a\text{-}RSx}$] y la parte almacenada en la base de datos de la aplicación es al menos una parte de [$ps_{1b\text{-}RPSx1}$] (que a este respecto está también asociada a DCx/2). Ventajosamente, en este ejemplo, des ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] requiere una personalización previa de [$ps_{1b\text{-}RPSx1}$] en la parte correspondiente de la base de datos de la aplicación (es decir en DCx/1 – RPSx/1) y su des ofuscación para uso en el cálculo de la clave de ofuscación que protege datos de personalización de seguridad de DCx/2.

En estas implementaciones DCx/1 son primeros dominios de código y DCx/2 son otros primeros dominios de código y DCx/2 son respectivamente vinculados en términos de seguridad a DCx/1 a través de la personalización de [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] en formato ofuscado en la parte correspondiente de la

base de datos de la aplicación (en el ejemplo anterior cada vinculación DCx/2 – DCx/1 depende de una parte de un parámetro de seguridad que está hard-coded (embebido) en el código de la aplicación de DCx/1 y de una parte de ese parámetro de seguridad que está almacenada en la base de datos de la aplicación).

Por tanto, dicha al menos parte del parámetro de seguridad [$ps_{1a\text{-}RSx}$] / [$ps_{1b\text{-}RPSx1}$] es requerida por el código de la aplicación de DCx/2 para des ofuscar adecuadamente [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] para uso, según definido, por el código de la aplicación de DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …). Por tanto, en esas implementaciones al menos una parte de un parámetro de seguridad disponible en una parte de la base de datos de la aplicación que está asociada a DCx/1 (es decir en DCx/1 – RPSx1) es requerida para habilitar DCx/2 para operación regular.

En un ejemplo particular, la parte [$ps_{1a\text{-}RSx}$] del parámetro de seguridad ha sido ofuscada usando una regla de ofuscación que está parcialmente hard-coded en el domino de código CDx/1 [ej. al menos parte de $ro_{1a\text{-}SRx}$] y parcialmente almacenada en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a DCx/1 [ej. al menos parte de $ro_{1b\text{-}RPSx1}$]. Por tanto en estas implementaciones al menos una parte de una regla de ofuscación disponible en una parte de la base de datos de la aplicación que está asociada a DCx/1 (es decir en DCx/1 – RPSx1) es requerida para habilitar DCx/2 para operación regular (es decir es requerida para des ofuscar una parte del parámetro de seguridad, que es requerido como parte de la clave para des ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$], por lo que la parte de la regla de ofuscación disponible en la parte correspondiente de la base de datos de la aplicación es requerida para habilitar DCx/2 para operación regular).

En un ejemplo particular, la parte [$ps_{1a\text{-}RSx}$] del parámetro de seguridad ha sido usada para calcular una red de checksums que está parcialmente hard-coded en el domino de código DCx/1 [ej. $ch_{1a\text{-}RSx}$] y parcialmente almacenada en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a DCx/1 [ej. $ch_{1b\text{-}RPSx1}$]. En este ejemplo, una verificación adecuada de la parte de la red de checksums disponible en una parte de la base de datos de la aplicación que está asociada a DCx/1 (es decir en DCx/1 – RPSx1) es requerida para habilitar DCx/2 para operación regular (ej. si la red de checksums no es verificada adecuadamente, el código de la aplicación de DCx/1 detendrá su ejecución, por lo que el parámetro de seguridad de DCx/1 no será obtenido, y DCx/2 no será habilitado para operación regular).

Ventajosamente, otro uno o más primeros dominios de código (ej. DCx/2) es vinculado en términos de seguridad a uno o más primeros dominios de código (ej. DCx/1) a través de la personalización de seguridad ([$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] almacenados en la base de datos de la aplicación en formato ofuscado), dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código (el parámetro de seguridad y/o regla de ofuscación y/o datos de checksums en DCx/1 referidos anteriormente) y que son requeridos para habilitar el otro uno o más primeros dominios de código para operación regular (ej. que es/son requeridos para des ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] para uso por DCx/2).

Conforme a algunas implementaciones cada uno de [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}rpsx1}$] son ofuscados usando una clave de ofuscación diferente. En un ejemplo particular:

- La clave usada para ofuscar [$ps_{2b\text{-}RPSx1}$] está constituida por un checksum de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad (ej. incluyendo una parte [$ps_{1a1\text{-}RSx}$] que está hard-coded (embebida) en el código de la aplicación de DCx/1 y una parte [$ps_{1b1\text{-}RPSx1}$] que es almacenada en formato ofuscado en la base de datos de la aplicación) y una parte de un identificador del dispositivo (ej. el MSISDN o un cálculo basado en el MSISDN, la dirección MAC, etc.).

- La clave usada para ofuscar [$ch_{2b\text{-}RPSx1}$] está constituida por un checksum de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad (ej. incluyendo una parte [$ps_{1a2\text{-}RSx}$] que está hard-coded (embebida) en el código de la aplicación de DCx/1 y una parte [$ps_{1b2\text{-}RPSx1}$] que es almacenada en formato ofuscado en la base de datos de la aplicación) y una parte de un identificador de dispositivo.

- La clave usada para ofuscar [$ro_{2b\text{-}RPSx1}$] está constituida por un checksum de la aplicación software protegida de dispositivo móvil, un parámetro de seguridad (ej. incluyendo una parte [$ps_{1a3\text{-}RSx}$] que está hard-coded (embebida) en el código de la aplicación de DCx/1 y una parte [$sp_{1b3\text{-}SPRx1}$] que es almacenada en formato ofuscado en la base de datos de la aplicación) y una parte de un identificador de dispositivo.

Para propósitos de test por el proveedor de servicios de personalización, un identificador de dispositivo de test – DID_{TEST} – puede ser usado como parte de la correspondiente clave de ofuscación.

Ventajosamente, en este ejemplo, des ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] requiere personalización previa de [$ps_{1b1\text{-}RPSx1}$], [$ps_{1b2\text{-}RPSx1}$] y [$ps_{1b3\text{-}RPSx1}$] (los cuales ej. pueden ser diferentes partes de [$ps_{1b\text{-}RPSx1}$]) en la parte correspondiente de la base de datos de la aplicación (es decir en DCx/1 – RPSx/1) y su des ofuscación para uso en el cálculo de la respectiva clave de ofuscación que protege los datos relativos de personalización de seguridad de DCx/2.

En estas implementaciones DCx/1 son primeros dominios de código y DCx/2 son otros primeros dominios de código y DCx/2 son respectivamente vinculados en términos de seguridad a DCx/1 a través de la personalización de [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] en formato ofuscado en la parte correspondiente de la base de datos de la aplicación. Cada vinculación DCx/2 – DCx/1 depende, en términos de [$ps_{2b\text{-}RPSx1}$] / [$ch_{2b\text{-}RPSx1}$] / [$ro_{2b\text{-}RPSx1}$], respectivamente del parámetro de seguridad [$ps_{1a1\text{-}RSx}$] & [$ps_{1b1\text{-}RPSx1}$] / [$ps_{1a2\text{-}RSx}$] & [$ps_{1b2\text{-}RPSx1}$] / [$ps_{1a3\text{-}RSx}$] & [$ps_{1b3\text{-}RPSx1}$].

Por tanto, dicho parámetro de seguridad [$ps_{1a1\text{-}RSx}$] & [$ps_{1b1\text{-}RPSx1}$] / [$ps_{1a2\text{-}RSx}$] & [$ps_{1b2\text{-}RPSx1}$] / [$ps_{1a3\text{-}RSx}$] & [$ps_{1b3\text{-}RPSx1}$] es requerido por el código de la aplicación de DCx/2 para respectivamente y adecuadamente des ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] para uso, según definido, por el código de la aplicación de DCx/2($f1_{DCx/2,}$ $f2_{DCx/2,}$ …). Por tanto, en esas implementaciones al menos una parte de parámetros de seguridad disponibles en una parte de la base de datos de la aplicación que está asociada a DCx/1 (es decir en DCx/1 – RPSx1) es requerida para habilitar DCx/2 para operación regular.

En un ejemplo particular, la parte [$ps_{1a1\text{-}RSx}$] / [$ps_{1a2\text{-}RSx}$] / [$ps_{1a3\text{-}RSx}$] del respectivo parámetro de seguridad ha sido ofuscada usando una o más reglas de ofuscación que están parcialmente hard-coded en el dominio de código CDx/1 y parcialmente almacenadas en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a CDx/1. Por tanto, en estas implementaciones al menos una parte de una o más reglas de ofuscación disponible en una parte de la base de datos de la aplicación que está asociada a DCx/1 (es decir en DCx/1 – RPSx1) es requerida para habilitar DCx/2 para operación regular (es decir es/son requeridas para des ofuscar una parte de los parámetros de seguridad, que son requeridos para calcular las claves de des ofuscación, tal que la(s) parte(s) de la(s) regla(s) de ofuscación disponibles en la parte correspondiente de la base de datos de la aplicación en relación a DCx/1 es/son requeridas para habilitar DCx/2 para operación regular.

En un ejemplo particular, las partes [$ps_{1a1\text{-}RSx}$] / [$ps_{1a2\text{-}RSx}$] / [$ps_{1a3\text{-}RSx}$] de los parámetros de seguridad han sido usadas para calcular una o más redes de checksums que son parcialmente hard-coded en el dominio de código DCx/1 y parcialmente almacenados en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a DCx/1. En este ejemplo, una verificación adecuada de la parte de las redes de checksums disponible en una parte de la base de datos de la aplicación que está asociad a DCx/1 (es decir en DCx/1 – RPSx1) es requerida para habilitar DCx/2 para operación regular (ej. si las redes de checksums no son adecuadamente verificadas, el código de la aplicación de DCx/1 detendrá su ejecución, por lo que el parámetro de seguridad de DCx/1 no será obtenido, y DCx/2 no será habilitado para operación regular.

Ventajosamente, otro uno o más primeros dominios de código (ej. DCx/2) es vinculado en términos de seguridad a uno o más primeros dominios de código (ej. DCx/1) a través de la personalización de seguridad ([$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] almacenados en la base de datos de la aplicación en formato ofuscado), dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código (el parámetro de seguridad y/o regla de ofuscación y/o datos de checksums en DCx/1 referidos anteriormente) y que son requeridos para habilitar el otro uno o más primeros dominios de código para operación regular (ej. que es/son requeridos para des ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}SPRx1}$] para uso por DCx/2).

La figura 2.b ha sido descrita anteriormente en relación a la generación de una aplicación software protegida de dispositivo móvil personalizada en seguridad, asociada al registro de personalización de seguridad RPS-I. La aplicación incluye varios dominios de código, cada uno agrupando una o más funciones de la aplicación software de dispositivo móvil que están asociadas al proveedor de servicios.

Como ya se ha detallado anteriormente en relación a la figura 2.b, conforme a algunas implementaciones la aplicación software de dispositivo móvil puede lograr el mismo nivel de funcionalidad usando [($f1_{DCk/1,}$ $f2_{DCk/1,}$ …) en DCk/1 y ($f1_{DCk/2,}$ $f2_{DCk/2,}$ …) en DCk/2] que usando [($f1_{DCl/1,}$ $f2_{DCl/1,}$ …) en DCl/1 y ($f1_{DCl/2,}$ $f2_{DCl/2,}$ …) en DCl/2], k y l en el rango de 1 a n.

En la implementación ilustrada en la figura 2.b, un proceso de ofuscación es aplicado por el software de protección de seguridad al código de la aplicación software de dispositivo móvil, y a parámetros de seguridad

del registro de personalización de seguridad, y a checksums de las redes de checksums del registro de personalización de seguridad.

Conforme a algunas implementaciones, una vez que la aplicación software protegida de dispositivo móvil ha sido generada, el proveedor de servicios de personalización verifica que la protección de seguridad ha sido aplicada adecuadamente, usando un parámetro de seguridad ($ps_{DCs\text{-}asignación}$] que está disponible en la parte correspondiente de la base de datos de la aplicación (como se ilustra en la figura 2.b) y que permite asignar para ejecución por un dispositivo móvil dado un conjunto dado de dominios de código, u otro diferente, de la siguiente forma:

- Si el parámetro de seguridad se establece en un valor dado asociado a DC2/1 y CD2/2 entonces la aplicación software protegida de dispositivo móvil puede usar las funciones de DC1, DC2/1 y CD2/2 durante su ejecución.

- Si el parámetro de seguridad se establece en un valor dado asociado a DC3/1 y DC3/2 entonces la aplicación software protegida de dispositivo móvil puede usar las funciones de DC1, DC3/1 y DC3/2 durante su ejecución.

- Si el parámetro de seguridad se establece en un valor dado asociado a DC4/1 y DC4/2 entonces la aplicación software protegida de dispositivo móvil puede usar las funciones de DC1, DC4/1 y DC4/2 durante su ejecución.

- Si el parámetro de seguridad se establece en un valor dado asociado a DCi/1 y DCi/2 entonces la aplicación software protegida de dispositivo móvil puede usar las funciones de DC1, DCi/1 y DCi/2 durante su ejecución.

- Si el parámetro de seguridad se establece en un valor dado asociado a DCn/1 y DCn/2 entonces la aplicación software protegida de dispositivo móvil puede usar las funciones de DC1, DCn/1 y DCn/2 durante su ejecución.

Conforme a algunas implementaciones el valor del parámetro de seguridad $sp_{CDs\text{-}asignación}$ es almacenado en formato ofuscado en la parte correspondiente de la base de datos de la aplicación. En un ejemplo particular el método para ofuscar $ps_{DCs\text{-}asignación}$ utiliza un parámetro de seguridad que está embebido en funciones de DC1. En otro ejemplo particular el método para ofuscar $ps_{DCs\text{-}asignación}$ utiliza un parámetro de seguridad que está embebido en una función de DC1 y al menos una parte de un identificador de dispositivo móvil. Durante su ciclo de vida una vez instalada en un dispositivo móvil, la aplicación software protegida de dispositivo móvil será capaz de obtener el referido parámetro de seguridad (/y el al menos parte del identificador de dispositivo móvil), para des ofuscar $ps_{DCs\text{-}asignación}$ e identificar los dominios de código que pueden ser usados durante la ejecución de la aplicación en dicho dispositivo móvil.

Conforme a algunas implementaciones, una vez que la aplicación software protegida de dispositivo móvil ha sido generada, puede ser testada para verificar que la protección de seguridad asociada a RPS-I ha sido aplicada adecuadamente. El test puede ser realizado usando ej. un dispositivo móvil de test o ej. un emulador de dispositivo móvil (el identificador de dispositivo móvil del dispositivo móvil de test o emulador es denominado como IDD_{TEST} en el contexto de las figuras 2.b, 2.c y 2.d).

Para realizar los test:

- El parámetro de seguridad $ps_{DCs\text{-}asignación}$ puede ser primero establecido al valor asociado a DC2/1 y DC2/2, tal que la aplicación software protegida de dispositivo móvil pueda usar las funciones de DC1, DC2/1 y DC2/2 durante su ejecución. El proceso de test debe verificar que cuando $P2_{RPS21}$ ha sido aplicada (es decir datos de RPS21 están almacenados en formato ofuscado en una parte de la base de datos de la aplicación que está asociada a DC2/1 y DC2/2), DC2/1 y CD2/2 están habilitados para operación regular;

- Una vez finalizados los test asociados a DC2/1 y CD2/2, el parámetro de seguridad $ps_{DCs\text{-}asignación}$ puede ser establecido al valor asociado a DC3/1 y CD3/2 para testar que cuando $P3_{RPS31}$ ha sido aplicada, DC3/1 y DC3/2 están habilitados para operación regular;

- Una vez finalizados los test asociados a DC(n-1)/1 y DC(n-1)/2, el parámetro de seguridad $ps_{DCs\text{-}asignación}$ puede ser establecido al valor asociado a DCn/1 y DCn/2 para testar que cuando Pn_{RPSn1} ha sido aplicada, DCn/1 y DCn/2 están habilitados para operación regular.

Cuando el parámetro de seguridad $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DCx/1 y DCx/2, conforme a algunas implementaciones la protección de seguridad personalizada ([$ps_{1b\text{-}RPSx1}$, $ch_{1b\text{-}RPSx1}$, $ro_{1b\text{-}RPSx1}$] almacenados en formato ofuscado en la parte correspondiente de la base de datos de la aplicación) asociada a DCx/1 y a IDD_{TEST}, es usada y testada de la siguiente forma:

- Una o más partes del parámetro de seguridad [$ps_{1a\text{-}RSx}$ / $ps_{1b\text{-}RPSx1}$] son usadas para validar que una solicitud para pre registrar un primer servicio, asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo apropiado y ha sido lanzada desde el código de dominio adecuado (CDx/1) con la personalización de seguridad adecuada. Durante dicho proceso las una o más partes de [$ps_{1a\text{-}RSx}$ / $ps_{1b\text{-}RPSx1}$] son des ofuscadas, y un cálculo basado en las unas o más partes des ofuscadas de [$ps_{1a\text{-}RSx}$ / $ps_{1b\text{-}RPSx1}$] es enviado al proveedor de servicios 1 para verificación. En el contexto del proceso de test, el dispositivo adecuado es el de identificador de dispositivo IDD_{TEST} y el proceso de verificación es realizado por un sistema de test del proveedor de servicios de personalización.

- Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RSx}$ / $ps_{1b\text{-}RPSx1}$] son usadas para proteger datos en ciertas partes de la base de datos de la aplicación software protegida de dispositivo móvil (cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DCx/1 y DCx/2). En una implementación particular, dichas otras una o más partes del parámetro de seguridad son usadas para proteger al menos parte de la parte de la base de datos de la aplicación que no está asociada a personalización de seguridad / asignación de dominios de código. Cuando la aplicación software protegida de dispositivo móvil recibe datos para almacenamiento en la al menos parte de la parte de la base de datos que no está asociada a personalización de seguridad / asignación de dominios de código, esos son cifrados usando las referidas otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RSx}$ / $ps_{1b\text{-}RPSx1}$], antes de ser almacenados en la correspondiente al menos parte de la parte de la base de datos de la aplicación.

  Cuando la aplicación software protegida de dispositivo móvil requiere el uso de datos almacenados en dicha al menos parte de la parte de la base de datos, las otras una o más partes de del parámetro de seguridad [$ps_{1a\text{-}RSx}$ / $ps_{1b\text{-}RPSx1}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar los datos en la base de datos, para uso. En el contexto del proceso de test el dispositivo usado es el de identificador de dispositivo IDD_{TEST}.

- Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RSx}$ / $ps_{1b\text{-}RPSx1}$] son el parámetro de seguridad que es parte de la clave de ofuscación usada para ofuscar [$ps_{2b\text{-}RPSx1}$], [$ch_{2b\text{-}RPSx1}$] y [$ro_{2b\text{-}RPSx1}$] (cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DCx/1 y DCx/2).

- La red de checksums [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSx1}$] es usada para verificar la integridad de partes del código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …).

  Cuando a aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSx1}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. En el contexto del proceso de test el dispositivo utilizado es el de identificador de dispositivo IDD_{TEST}.

  - En una implementación alternativa:
    - una o más partes de la red de checksums [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSx1}$] son usadas para verificar la integridad de partes del código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un primer valor;

    - otras una o más partes de la red de checksums [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSx1}$] son usadas para verificar la integridad de otras partes del código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) y de al menos partes de otros uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un segundo valor;

    - otras una o más partes de la red de checksums [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSx1}$] son usadas para verificar la integridad de otras partes del código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) y de al menos partes de otros uno o más parámetros de seguridad embebidos en el código de la

aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un enésimo valor;

Ventajosamente, dependiendo del valor establecido en $ps_{DCs\text{-}asignación}$, una parte(s) diferente de [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSx1}$] puede ser usada en la verificación de integridad. El proceso de test puede testar todos los posibles valores, usando el identificador de dispositivo IDD_{TEST} como dispositivo utilizado.

- La regla de ofuscación [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSx1}$] es usada para ofuscar parte del código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …) junto con parte [$ps_{1a\text{-}RSx}$, $ps_{3\text{-}RSx,}$ $ps_{4\text{-}RSx}$ …, $ps_{g\text{-}RSx}$] y parte de [$ch_{1a\text{-}RSx}$, $ch_{3\text{-}RSx,}$ $ch_{4\text{-}RSx}$ …, $ch_{g\text{-}RSx}$] embebidos en el código de la aplicación de las funciones DCx/1($f1_{DCx/1}$, $f2_{DCx/1,}$ …).

  Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha parte referida del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSx1}$]. En el contexto del proceso de test el dispositivo utilizado es el de identificador de dispositivo IDD_{TEST}.

  - En una implementación alternativa al menos una función dada en CDx/1 ($fi_{DCx/1}$) es codificada g-veces en DCx/1, las instrucciones de cada réplica de la función siendo equivalentes en términos de funcionalidad. En esta implementación alternativa, parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la primera réplica es ofuscada usando una o más partes de la regla de ofuscación [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSx1}$], …., parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la G-réplica es ofuscada usando otras una o más partes de la regla de ofuscación [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSx1}$]. También:

    - La una o más partes de la regla de ofuscación [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSx1}$] son usadas para des ofuscar la parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la primera réplica de la función cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un primer valor;

    - Las otras una o más partes de la regla de ofuscación [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSx1}$] son usadas para des ofuscar la parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la G-réplica de la función cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un G valor;

    Ventajosamente, dependiendo del valor establecido en $ps_{DCs\text{-}asignación}$, diferentes una o más partes de [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSx1}$] son usadas en la des ofuscación de la correspondiente parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la correspondiente réplica de la al menos una función $fi_{DCx/1}$ dada. El proceso de test puede testear todos los posibles valores, usando el identificador de dispositivo IDD_{TEST} como dispositivo usado.

También, cuando el parámetro de seguridad $ps_{DCs\text{-}asignación}$ se establece al valor asociado a DCx/1 y DCx/2, conforme a algunas implementaciones la personalización de seguridad personalizada ([$ps_{2b\text{-}RPSx1}$, $ch_{2b\text{-}RPSx1}$, $ro_{2b\text{-}RPSx1}$] almacenados en formato ofuscado en la correspondiente parte de la base de datos de la aplicación) asociada a DCx/2 y a IDD_{TEST}, es usada a testada de la siguiente forma:

- Una o más partes del parámetro de seguridad [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] son usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DCx/2 a partir de un pre registro previo con éxito del primer servicio), asociada al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo apropiado y ha sido lanzada desde el dominio de código adecuado (DCx/2) con la personalización de seguridad adecuada. Durante dicho proceso las una o más partes de [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] son des ofuscadas, y un cálculo basado en las des ofuscadas una o más partes de [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] es enviado al proveedor de servicios 1 para verificación. En el contexto del proceso de test, el dispositivo apropiado es el de identificador de dispositivo IDD_{TEST} y el proceso de verificación es realizado por un sistema de test del proveedor de servicios de personalización.

  Conforme a algunas implementaciones un PIN (Personal Identification Number) es seleccionado por el usuario durante el proceso de registrar un primer servicio del proveedor de servicios 1 en la aplicación software protegida de dispositivo móvil, y datos almacenados en la base de datos de la aplicación software protegida de dispositivo móvil durante la fase de pre registro son usados para autenticar el registro del PIN seleccionado en el sistema del proveedor de servicios 1.

- Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] son usadas para proteger ciertos datos sensibles no estructurados antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil (ej. para proteger claves / datos sensibles necesarios para que la aplicación software protegida de dispositivo móvil calcule credenciales dinámicas asociadas a servicios provistos por el proveedor de servicios 1; ej. protección de claves de sesión), cuando psDCs-asignación es establecido al valor asociado a DCx/1 y DCx/2. Conforme a algunas implementaciones, los datos sensibles no estructurados son cifrados por el proveedor de servicios 1, o por un tercero en nombre del proveedor de servicios 1, utilizando las otras una o más partes de [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] y enviados a la aplicación software protegida de dispositivo móvil para almacenamiento en la base de datos de la aplicación.

  Cuando la aplicación software protegida de dispositivo móvil requiere el uso de al menos parte de los datos sensibles no estructurados, las otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar la al menos parte de los datos sensibles no estructurados almacenados, para uso. En el contexto del proceso de test el dispositivo usado es el de identificador de dispositivo IDD_{TEST}.

- Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] son usadas para ofuscar ciertos datos sensibles, en el contexto de la ejecución de algunas instrucciones de código de DCx/2, para evitar que sean expuestos en claro en una o más memorias de trabajo del dispositivo móvil, cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DCx/1 y DCx/2.

  Conforme a algunas implementaciones ciertos datos sensibles (ej. una o más claves) son ofuscadas antes de ser temporalmente almacenadas en una o más memorias de trabajo del dispositivo móvil en el contexto de la ejecución de ciertas instrucciones de código relativas a DCx/2 por una o más dispositivos de procesamiento en el dispositivo móvil, tal que dichos datos sensibles no sean expuestos en claro en las memorias de trabajo.

  En un ejemplo particular la regla de ofuscación usa las otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] y es relativa a mezclar los datos sensibles con conjuntos de datos no-útiles, para uso temporal en las unas o más memorias de trabajo.

  Cuando, durante la ejecución de ciertas instrucciones de código de DCx/2, los uno o más dispositivos de procesamiento requieren usar los datos sensibles ofuscados previamente almacenados en las una o más memorias de trabajo, utilizan las otras una o más partes de [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] y la regla de ofuscación para obtener los datos adecuados para el relativo proceso de cálculo.

  La lógica anterior puede ser repetida conforme a la programación de las funciones de DCx/2 tal que las otras una o más partes de [$ps_{2a\text{-}RSx}$ / $ps_{2b\text{-}RPSx1}$] servirán para evitar que ciertos datos sensibles sean expuestos en claro en las una o más memorias de trabajo del dispositivo móvil durante los sucesivos cálculos por los uno o más dispositivos de procesamiento que usan esos datos sensibles.

  En el contexto del proceso de test el dispositivo utilizado es el de identificador de dispositivo IDD_{TEST}.

- La red de checksums [$ch_{2a\text{-}RSx}$ / $ch_{2b\text{-}RPSx1}$] es usada para verificar la integridad de partes del código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …).

  Cuando la aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{2a\text{-}RSx}$ / $ch_{2b\text{-}RPSx1}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. En el contexto del proceso de test el dispositivo utilizado es el de identificador de dispositivo IDD_{TEST}.

  - En una implementación alternativa:

    - una o más partes de la red de checksums [$ch_{2a\text{-}SRx}$ / $ch_{2b\text{-}SPRx1}$] son usadas para verificar la integridad de partes del código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un primer valor;

- otras una o más partes de la red de checksums [$ch_{2a\text{-}SRx}$ / $ch_{2b\text{-}SPRx1}$] son usadas para verificar la integridad de otras partes del código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) y de al menos partes de otros uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un segundo valor;

- otras una o más partes de la red de checksums [$ch_{2a\text{-}SRx}$ / $ch_{2b\text{-}SPRx1}$] son usadas para verificar la integridad de otras partes del código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) y de al menos partes de otros uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un enésimo valor;

Ventajosamente, dependiendo del valor establecido en $ps_{DCs\text{-}asignación}$, una parte diferente de [$ch_{2a\text{-}RSx}$ / $ch_{2b\text{-}RPSx1}$] puede ser usada in la verificación de integridad. El proceso de test puede testear todos los valores posibles, usando el identificador de dispositivo IDD_{TEST} como dispositivo utilizado.

- La regla de ofuscación [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSx1}$] es usada para ofuscar parte del código de la aplicación de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …) junto con parte de los [$ps_{2a\text{-}RSx}$, $ps_{(g+1)\text{-}RSx,}$ $ps_{(g+2)\text{-}RSx}$ …, $ps_{m\text{-}RSx}$] y parte de los [$ch_{2a\text{-}RSx}$, $ch_{(g+1)\text{-}RSx,}$ $ch_{(g+2)\text{-}RSx}$ …, $ch_{m\text{-}RSx}$] embebidos en el código de la aplicaciones de las funciones DCx/2($f1_{DCx/2}$, $f2_{DCx/2,}$ …).

  Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha referida parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSx1}$]. En el contexto del proceso de test el dispositivo utilizado es el de identificador de dispositivo IDD_{TEST}.

  - En una implementación alternativa al menos una función dada en DCx/2 ($fi_{DCx/2}$) es codificada h-veces en DCx/2, siendo las instrucciones de cada réplica de la función equivalentes en términos de funcionalidad. En esta implementación alternativa, parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la primera replica son ofuscados usando una o más partes de la regla de ofuscación [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSx1}$], …., parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la H-replica son ofuscados usando otras una o más partes de la regla de ofuscación [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSx1}$]. También:

    - Las una o más partes de la regla de ofuscación [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSx1}$] son usadas para des ofuscar la parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la primera replica de la función cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un primer valor;

    - Las otras una o más partes de la regla de ofuscación [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSx1}$] son usadas para des ofuscar la parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la H-replica de la función cuando un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un H-valor;

    Ventajosamente, dependiendo del valor establecido en $ps_{DCs\text{-}asignación}$, diferentes una o más partes de [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSx1}$] son usadas en la des ofuscación de la correspondiente parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la correspondiente réplica de la al menos una función $fi_{DCx/2}$ dada. El proceso de test puede testear todos los posibles valores, usando el identificador de dispositivo IDD_{TEST} como dispositivo usado.

Conforme a algunas implementaciones, tras un test con éxito la aplicación software protegida de dispositivo móvil es almacenada en la base de datos (BD) del proveedor de servicios de personalización que está asociada a aplicaciones software protegidas de dispositivo móvil, en relación a los datos de personalización de seguridad que habilitan los uno o más primeros dominios de código para operación regular y a los registros de personalización de seguridad (incluyendo RPS-I).

Conforme a algunas implementaciones, el proceso de test puede también chequear que cuando una personalización/asignación de seguridad errónea es aplicada, DCx/1 y/o DCx/2 no es/son habilitados para operación regular. La figura 2.e ilustra un conjunto de registros de personalización de seguridad (RPSxVD, x= 2, 3, …, n) con valores por defecto (/erróneos), que pueden ser usados para propósitos de test. En el proceso de test, el parámetro de seguridad $ps_{DCs\text{-}asignación}$ puede también ser establecido con valores por defecto (/erróneos).

La figura 2.f ilustra una personalización de seguridad que usa los valores por defecto, una vez que ha sido aplicada a la aplicación software protegida de dispositivo móvil. Los siguientes son algunos ejemplos para testear que la personalización de seguridad basada en esos valores por defecto (/erróneos) no habilita la aplicación software protegida de dispositivo móvil para operación regular:

- El valor de $ps_{DCs\text{-}asignación}$ no corresponde a un parámetro válido para asignar un DCx/1 y CDx/2 dados, o el parámetro es válido pero no está adecuadamente ofuscado, por lo que la reacción de autoprotección programada para tal escenario será aplicada por la aplicación software protegida de dispositivo móvil.

- El valor de $ps_{DCs\text{-}asignación}$ es correcto y está correctamente ofuscado, y es relativo a la asignación de DCx/1 y DCx/2:

    - En un entorno de test, $ps_{1b\text{-}RPSxVD}$ ha sido personalizado en formato ofuscado en la parte de la base de datos de la aplicación asociada a CDx/1. Cuando se usa $ps_{1b\text{-}RPSxVD}$ la validación asociada a la solicitud para pre registrar un primer servicio en la aplicación software protegida de dispositivo móvil fallará, y el pre registro no será realizado; también, la clave calculada para des ofuscar datos de personalización de seguridad DCx/2 no será correcta, por lo que los valores des ofuscados no serán correctos y una o más reacciones de auto reacción programadas para dicho escenario serán realizadas, según aplique cuando se ejecuten instrucciones de código de DCx/2 que usen esos valores, por la aplicación software protegida de dispositivo móvil.

    - En un entorno de test, $ch_{1b\text{-}RPSxVD}$ ha sido personalizada en formato ofuscado en la parte de la base de datos de la aplicación asociada a DCx/1. En este test [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSxVD}$] es usado en la verificación de integridad. Si [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSxVD}$] es comparado con el calculado por la aplicación software protegida de dispositivo móvil, la verificación fallará y la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

        - En la implementación alternativa, referida anteriormente en relación a la figura 2.b, en un entorno de test, $ch_{1b\text{-}RPSxVD}$ ha sido personalizadas en formato ofuscado en la parte de la base de datos de la aplicación asociada a DCx/1. En este test el valor establecido en $ps_{DCs\text{-}asignación}$ hace que una o más partes dadas de [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSxVD}$] sean usadas en la verificación de integridad. Si las una o más partes dadas de [$ch_{1a\text{-}RSx}$ / $ch_{1b\text{-}RPSxVD}$] son comparadas con la calculada por la aplicación software protegida de dispositivo móvil, la verificación fallará y la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

    - En un entorno de test, $ro_{1b\text{-}RPSxVD}$ has sido personalizada en formato ofuscado en una parte de la base de datos de la aplicación asociada a DCx/1. En este test [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSxVD}$] es usada por la aplicación software protegida de dispositivo móvil para des ofuscar la correspondiente parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas, tal que el proceso de des ofuscación no será correcto y la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

        - En una implementación alternativa, referida anteriormente en relación a la figura 2.b, en un entorno de test, $ro_{1b\text{-}RPSxVD}$ ha sido personalizada en formato ofuscado en una parte de la base de datos de la aplicación asociada a DCx/1. En este test, el valor establecido en $ps_{DCs\text{-}asignación}$ hace que una o más partes dadas de [$ro_{1a\text{-}RSx}$ / $ro_{1b\text{-}RPSxVD}$] sean usadas por la aplicación software protegida de dispositivo móvil para des ofuscar la correspondiente parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la correspondiente réplica de la al menos una función $fi_{DCx/1}$ dada, por lo que el proceso de des ofuscación no será correcto y la reacción de auto protección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

    - En un entorno de test, el identificador de dispositivo del dispositivo donde la aplicación ha sido instalada es diferente que IDD_{TEST}, por lo que la clave calculada por la aplicación software protegida de dispositivo móvil no será la adecuada para des ofuscar correctamente los datos personalizados de seguridad almacenados en la parte de la base de datos de la aplicación asociada a DCx/1, por lo que la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

- En un entorno de test $ps_{2b\text{-}RPSxVD}$ ha sido personalizada en formato ofuscado en la parte de la base de datos de la aplicación asociada a DCx/2. Cuando se usa $ps_{2b\text{-}RPSxVD}$ la validación asociada a la solicitud para registrar el primer servicio referido anteriormente en la aplicación software protegida de dispositivo móvil fallará, y el registro no será realizado; también, los datos sensibles no estructurados protegidos almacenados en la base de datos de la aplicación software protegida de dispositivo móvil no serán descifrados adecuadamente, por lo que los valores serán incorrectos cuando se utilicen.

- En un entorno de test $ch_{2b\text{-}RPSxVD}$ ha sido personalizado en formato ofuscado en una parte de la base de datos de la aplicación asociada a DCx/2. En este test [$ch_{2a\text{-}RSx}$ / $ch_{2b\text{-}RPSxVD}$] es usado en la verificación de integridad. Si [$ch_{2a\text{-}RSx}$ / $ch_{2b\text{-}RPSxVD}$] es comparado con el calculado por la aplicación software protegida de dispositivo móvil, la verificación fallará y la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

  - En la implementación alternativa, referida anteriormente en relación a la figura 2.b, en un entorno de test $ch_{2b\text{-}RPSxVD}$ ha sido personalizada en formato ofuscado en la parte de la base de datos de la aplicación asociada a DCx/2. En este test el valor establecido en $ps_{DCs\text{-}asignación}$ hace que una o más partes dadas de [$ch_{2a\text{-}RSx}$ / $ch_{2b\text{-}RPSxVD}$] sean usadas en la verificación de integridad. Si las una o más partes dadas de [$ch_{2a\text{-}RSx}$ / $ch_{2b\text{-}RPSxVD}$] son comparadas con la calculada por la aplicación software protegida de dispositivo móvil, la verificación fallará y la reacción de auto protección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

- En un entorno de test, $ro_{2b\text{-}RPSxVD}$ ha sido personalizada en formato ofuscado en la parte de la base de datos de la aplicación asociada a DCx/2. En este test [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSxVD}$] es usada por la aplicación software protegida de dispositivo móvil para des ofuscar la parte correspondiente del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas, por lo que el proceso de des ofuscación no será correcto y la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

  - En la implementación alternativa, referida anteriormente en relación a la figura 2.b, en un entorno de test, $ro_{2b\text{-}RPSxVD}$ ha sido personalizada en formato ofuscado en la parte de la base de datos de la aplicación asociada a DCx/2. En este test, el valor establecido en $ps_{DCs\text{-}asignación}$ hace que una o más partes dadas de [$ro_{2a\text{-}RSx}$ / $ro_{2b\text{-}RPSxVD}$] sea usada por la aplicación software protegida de dispositivo móvil para des ofuscar la correspondiente parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la correspondiente réplica de la al menos una función $fi_{DCx/2}$ dada, por lo que el proceso de des ofuscación no será correcto y la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

- En un entorno de test, al menos parte de $ps_{1b\text{-}RPSxVD}$ será usado por la aplicación software protegida de dispositivo móvil para calcular la clave para des ofuscar los datos personalizados de seguridad almacenados en la parte de la base de datos de la aplicación asociada a DCx/2. Como se ha detallado anteriormente, usando $ps_{1b\text{-}RPSxVD}$, $ch_{1b\text{-}RPSxVD}$, $ro_{1b\text{-}RPSxVD}$, una o más reacciones de autoprotección definidas ocurrirán y la referida clave para des ofuscar $ps_{2b\text{-}RPSxVD}$, $ch_{2b\text{-}RPSxVD}$, $ro_{2b\text{-}RPSxVD}$ no podrá ni siquiera ser calculada.

- En un entorno de test, el identificador de dispositivo del dispositivo donde la aplicación ha sido instalada es diferente que IDD_{TEST}, por lo que la clave calculada por la aplicación software protegida de dispositivo móvil no será la adecuada para des ofuscar correctamente los datos personalizados de seguridad almacenados en la parte de la base de datos de la aplicación asociada a DCx/2, por lo que la reacción de autoprotección programada para ese escenario será realizada por la aplicación software protegida de dispositivo móvil.

- Etc.

Otros valores por defecto de personalización de seguridad pueden ser usados para testar más las diferentes posibles asignaciones de dominios de código y configuraciones de seguridad de la aplicación software protegida de dispositivo móvil.

Las reacciones de autoprotección aplicadas pueden ser diversas (ej. la aplicación detiene su ejecución; la aplicación reacciona haciendo que la base de datos de la aplicación sea borrada y/o enviando un mensaje de aviso a través del dispositivo móvil al proveedor de servicios de personalización y/o al correspondiente proveedor de servicios, etc.), y una o más reacciones de autoprotección pueden ser aplicadas a cada medida de protección de la aplicación software protegida de dispositivo móvil.

Una vez que el proceso de test ha finalizado, como se describe en relación a la figura 1 la aplicación software protegida de dispositivo móvil es almacenada en la base de datos (BD) asociada a aplicaciones software protegidas de dispositivo móvil, en relación a los datos de personalización de seguridad que habilitan los uno o más primeros dominios de código para operación regular y a los registros de personalización de seguridad (incluyendo RPS-I).

Después, el módulo de personalización de seguridad obtiene usando uno o más dispositivos de procesamiento la aplicación software protegida de dispositivo móvil de la base de datos. Conforme a algunas implementaciones la aplicación protegida es obtenida sin ningún dato asociado a la personalización de seguridad que habilita los uno o más primeros dominios de código para operación regular, por lo que la aplicación obtenida es una aplicación software protegida de dispositivo móvil no personalizada en seguridad. La aplicación software protegida de dispositivo móvil no personalizada en seguridad está en un estado de personalización de seguridad pendiente, dicho estado de personalización de seguridad pendiente deshabilitando los uno o más primeros dominios de código para operación regular.

Como también se describe en la figura 1, la aplicación software protegida de dispositivo móvil es enviada en un estado de seguridad no-personalizada desde el proveedor de servicios de personalización a un servidor de distribución de una entidad a cargo de distribuir la aplicación y dicha aplicación es almacenada en una o más memorias del servidor de distribución de dicha entidad. Conforme a algunas implementaciones el servidor de distribución es relativo a uno o más de los servidores asociados a un mercado de distribución de aplicaciones o una tienda de aplicaciones tales como Google Play Store o Apple Store.

Después, a partir de interacción del usuario el teléfono móvil del usuario solicita una aplicación software de dispositivo móvil al servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada.

En el siguiente paso el dispositivo móvil del usuario recibe desde el servidor de distribución y subsecuentemente instala usando uno o más dispositivos de procesamiento en el dispositivo móvil la aplicación software protegida de dispositivo móvil no personalizada en seguridad, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código están deshabilitados para operación regular.

Ventajosamente, cuando la aplicación software protegida de dispositivo móvil es descargada desde el servidor de distribución y es instalada en el dispositivo móvil del usuario, la aplicación software protegida de dispositivo móvil está en un estado de seguridad no-personalizada donde los uno o más primeros dominios de código están deshabilitados para operación regular, por lo que la aplicación se auto protegerá contra intentos de ej. realizar ejecuciones de código según se ha explicado extensamente en conexión a algunas de las figuras previas.

Las figuras 2.g a 2.l son relativas a algunas implementaciones donde la aplicación software protegida de dispositivo móvil instalada en el dispositivo móvil del usuario 1 es personalizada en términos de seguridad usando un primer registro de personalización de seguridad de ciclo de vida, y la aplicación software protegida de dispositivo móvil instada en el dispositivo móvil del usuario 2 es personalizada en términos de seguridad usando un segundo registro de personalización de seguridad de ciclo de vida, ambos el primer y el segundo registros de personalización de seguridad de ciclo de vida siendo diferentes que el registro de personalización de seguridad de inicialización (RPS-I en los ejemplos anteriores).

En estas implementaciones cada registro de personalización de seguridad de ciclo de vida está asociado en el sistema del proveedor de servicios de personalización a un conjunto de primeros y segundos dominios de código de la siguiente forma:

- Cada uno de los RPS2j (j= 2 to N), está asociado a los primeros dominios de código DC2/1 y DC2/2 y al segundo dominio de código CD1;

- Cada uno de los RPS3j (j= 2 to N), está asociado a los primeros dominios de código DC3/1 y DC3/2 y al segundo dominio de código CD1;

- Cada uno de los RPS4j (j= 2 to N), está asociado a los primeros dominios de código DC4/1 y DC4/2 y al segundo dominio de código CD1;

- Cada uno de los RPSij (j= 2 to N), está asociado a los primeros dominios de código DCi/1 y DCi/2 y al segundo dominio de código CD1;

- Cada uno de los RPSnj (j= 2 to N), está asociado a los primeros dominios de código DCn/1 y DCn/2 y al segundo dominio de código CD1;

y la asociación es almacenada en la base de datos asociada a aplicaciones software protegidas de dispositivo móvil.

Como se describe en relación al paso (8) de la figura 1, el dispositivo móvil del usuario envía una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada, la solicitud incluyendo un identificador del dispositivo móvil del usuario ($IDD_{USUARIO}$). En el paso (9) el proveedor de servicios de personalización recibe la solicitud desde el dispositivo móvil del usuario y en el paso (10) uno o más dispositivos de procesamiento del proveedor de servicios de personalización asignan un registro de personalización de seguridad de ciclo de vida al dispositivo móvil del usuario ($IDD_{USUARIO}$) en relación a la aplicación software protegida de dispositivo móvil.

La figura 2.g es primero relativa a un escenario donde la aplicación software protegida de dispositivo móvil es instalada en el dispositivo móvil del usuario 1 (con $IDD_{USUARIO1}$), y los pasos (8), (9) y (10) tienen lugar en relación a dicho dispositivo móvil del usuario 1. En el ejemplo ilustrado en la figura 2.g el registro de personalización de seguridad de ciclo de vida asignado por el módulo de personalización de seguridad al dispositivo móvil del usuario 1 es RPS43, que como se ha referido anteriormente está asociado a DC4/1, DC4/2 y DC1. Todavía en el paso (10) la asignación del registro de personalización de seguridad de ciclo de vida RPS43 al dispositivo móvil del usuario 1 y a la aplicación software protegida de dispositivo móvil es almacenada en la base de datos asociada a aplicaciones software protegidas de dispositivo móvil.

En más detalle, conforme a algunas implementaciones el módulo de personalización de seguridad puede realizar las siguientes asignaciones y preparación de datos en el paso (10) (algunos de los procesos de preparación de datos pueden también ser realizados en una fase posterior, antes de enviar los datos a la aplicación software protegida de dispositivo móvil), in relación al dispositivo móvil del usuario 1 y a la personalización de seguridad:

- Asignación de RPS43 en el contexto del proceso de personalización de seguridad en curso, asociado a DC4/1, DC4/2 y DC1 y a $IDD_{USUARIO1}$;

- Asignar a $ps_{DCs\text{-}asignación}$ un valor de dato asociado a DC4/1 y DC4/2 tal que, una vez personalizado en seguridad, la aplicación software protegida de dispositivo móvil use DC4/1, DC4/2 y DC1 durante su ejecución. En estas implementaciones el valor de dato está ofuscado usando un método que usa un parámetro de seguridad que está embebido en una función de DC1 y al menos parte del $IDD_{USUARIO1}$.

- Ofuscación de [$ps_{1b\text{-}RPS43}$, $ro_{1b\text{-}RPS43}$, $ch_{1b\text{-}RPS43}$] usando un algoritmo de ofuscación y la clave de ofuscación para proteger datos de personalización de seguridad CD4/1, como se ilustra en la figura 2.g (en este proceso de personalización de seguridad x = 4). En estas implementaciones:

  - Los primeros 10 dígitos de $IDD_{USUARIO1}$ son parte de la clave de ofuscación;

  - [$ps_{1a\text{-}RS4}$, $ps_{1b\text{-}RPS43}$] se convierten en las dos partes del mismo parámetro de seguridad:

    - Una o más partes de [$ps_{1a\text{-}RS4}$, $ps_{1b\text{-}RPS43}$] serán usadas para validar que una solicitud para pre registrar un primer servicio, asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 1 (con $IDD_{USUARIO1}$) y ha sido lanzada desde DC4/1 con la personalización de seguridad adecuada;

    - Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$] serán usadas para proteger datos en ciertas partes de la base de datos de la aplicación software protegida de dispositivo móvil (en este contexto, ciertas partes asociadas a DC4/1 y DC4/2). En estas implementaciones, dichas otras una o más partes del parámetro de seguridad son usadas

para proteger al menos parte de la parte de la base de datos de la aplicación que no está asociada a personalización / asignación de seguridad de dominios de código.

Cuando la aplicación software protegida de dispositivo móvil recibe datos para almacenamiento en la al menos parte de la parte de la base de datos que no está asociada a personalización / asignación de seguridad de dominios de código, esos son cifrados usando las referidas otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$], antes de ser almacenados en la correspondiente al menos parte de la parte de la base de datos de la aplicación.

- Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$] son asignadas como el parámetro de seguridad que es parte de la clave de ofuscación usada para ofuscar [$ps_{2b\text{-}RPS43}$], [$ch_{2b\text{-}RPS43}$] y [$ro_{2b\text{-}RPS43}$].

- [$ch_{1a\text{-}SR4}$, $ch_{1b\text{-}SPR43}$] se convierten en las dos partes de la misma red de checksums, que será usada para verificar la integridad de partes del código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …).

  - En estas implementaciones $ch_{1b\text{-}RPS43} = ch_{1b\text{-}RPS41}$;

  - Conforme a algunas implementaciones alternativas $ch_{1b\text{-}RPS43} = ch_{1b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la red de checksums [$ch_{1a\text{-}RS4}$ / $ch_{1b\text{-}RPS43}$] serán usadas para verificar la integridad de partes del código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …);

- [$ro_{1a\text{-}RS4}$, $ro_{1b\text{-}RPS43}$] se convierten en las dos partes de la misma regla de ofuscación, que es usada para ofuscar parte del código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …) junto con parte de los [$ps_{1a\text{-}RS4}$, $ps_{3\text{-}RS4,}$ $ps_{4\text{-}RS4}$ …, $ps_{i\text{-}RS4}$] y parte de los [$ch_{1a\text{-}RS4}$, $ch_{3\text{-}RS4,}$ $ch_{4\text{-}RS4}$ …, $ch_{i\text{-}RS4}$] embebidos en el código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …).

  - En estas implementaciones $ro_{1b\text{-}RPS43} = ro_{1b\text{-}RPS41}$;

  - Conforme a algunas implementaciones alternativas $ro_{1b\text{-}RPS43} = ro_{1b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{1a\text{-}RS4}$ / $ro_{1b\text{-}RPS43}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la réplica de la función $fi_{DC4/1}$ en DC4/1 que está asociada al valor dado del parámetro.

- Ofuscación de [$ps_{2b\text{-}RPS43}$, $ro_{2b\text{-}RPS43}$, $ch_{2b\text{-}RPS43}$] usando un algoritmo de ofuscación y la clave de ofuscación para proteger datos de personalización de seguridad DC4/2, como se ilustra en la figura 2.g (en este proceso de personalización de seguridad x = 4). En estas implementaciones:

  - El parámetro de seguridad que es parte de la clave de ofuscación está constituido por al menos parte de [$ps_{1a\text{-}RS4}$] y al menos parte de [$ps_{1b\text{-}RPS43}$]. Los primeros 10 dígitos de $IDD_{USUARIO1}$ son también parte de la clave de ofuscación;

  - [$ps_{2a\text{-}RS4}$, $ps_{2b\text{-}RPS43}$] se convierten en las dos partes del mismo parámetro de seguridad:

    - Una o más partes de [$ps_{2a\text{-}RS4}$, $ps_{2b\text{-}RPS43}$] serán usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC4/2 tras un pre registro previo con éxito del primer servicio), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 1 (con $IDD_{USUARIO1}$) y ha sido lanzada desde DC4/2 con la personalización de seguridad adecuada;

    - Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] serán usadas para proteger ciertos datos sensibles no estructurados antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1 (ej.

para proteger claves/datos sensibles necesarios para que la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1 calcule credenciales dinámicas asociadas a servicios provistos por el proveedor de servicios 1; ej. protección de claves de sesión), cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DC4/1 y DC4/2.

- Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] serán usadas por la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1 para ofuscar ciertos datos sensibles, en el contexto de la ejecución de algunas instrucciones de código DC4/2, para evitar que sean expuestas en claro en una o más memorias de trabajo del dispositivo móvil, cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DC4/1 y DC4/2.

  - [$ch_{2a\text{-}RS4}$, $ch_{2b\text{-}RPS43}$] se convierten en las dos partes de la misma red de checksums, que será usada para verificar la integridad de partes del código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …).

    - En estas implementaciones $ch_{2b\text{-}RPS43} = ch_{2b\text{-}RPS41}$;

    - Conforme a algunas implementaciones alternativas $ch_{2b\text{-}RPS43} = ch_{2b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la red de checksums [$ch_{2a\text{-}RS4}$ / $ch_{2b\text{-}RPS43}$] serán usadas para verificar la integridad de partes del código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …);

  - [$ro_{2a\text{-}RS4}$, $ro_{2b\text{-}RPS43}$] se convierten en las dos partes de la misma regla de ofuscación, que son usadas para ofuscar parte del código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …) junto con parte de los [$ps_{2a\text{-}RS4}$, $ps_{(i+1)\text{-}RS4,}$ $ps_{(i+2)\text{-}RS4}$ …, $ps_{q\text{-}RS4}$] y parte de los [$ch_{2a\text{-}RS4}$, $ch_{(i+1)\text{-}RS4,}$ $ch_{(i+2)\text{-}RS4}$ …, $ch_{q\text{-}RS4}$] embebidos en el código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …).

    - En estas implementaciones $ro_{2b\text{-}RPS43} = ro_{2b\text{-}RPS41}$;

    - Conforme a algunas implementaciones alternativas $ro_{2b\text{-}RPS43} = ro_{2b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{2a\text{-}RS4}$ / $ro_{2b\text{-}RPS43}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la réplica de la función $fi_{DC4/2}$ en DC4/2 que está asociada al valor dado del parámetro.

Estas asignaciones y datos preparados son almacenados en la base de datos asociada a aplicaciones software protegidas de dispositivo móvil, en relación al dispositivo móvil del usuario 1, la aplicación software protegida de dispositivo móvil y el proceso de personalización de seguridad.

En el paso (11) de la figura 1 al menos parte del registro de personalización de seguridad de ciclo de vida asignado, y la asociación al dispositivo móvil del usuario y a la aplicación software protegida de dispositivo móvil es enviada al proveedor de servicios correspondiente tal que pueda usar al menor parte de ello en el contexto de ciertos procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil. Conforme a algunas implementaciones (en relación a la figura 2.g) al menos parte de las asignaciones y datos asociados al dispositivo móvil del usuario 1 y a la personalización de seguridad de la aplicación software protegida de dispositivo móvil son enviados al proveedor de servicios 1 para almacenamiento y/o para uso de al menos parte de ello en el contexto de ciertos procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil asociada al dispositivo móvil del usuario 1. En un ejemplo particular:

- Las una o más partes de [$ps_{1a\text{-}RS4}$, $ps_{1b\text{-}RPS43}$] que serán usadas para validar que una solicitud para pre registrar un primer servicio, asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 1 (con $IDD_{USUARIO1}$) y ha sido lanzada desde DC4/1 con la personalización de seguridad adecuada y;

- Las una o más partes de [$ps_{2a\text{-}RS4}$, $ps_{2b\text{-}RPS43}$] que serán usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC4/2 tras un pre registro previo con éxito del primer servicio), asociado al proveedor de servicios 1, en la

aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 1 (con $IDD_{USUARIO1}$) y ha sido lanzada desde DC4/2 con la personalización de seguridad adecuada;

son enviadas al proveedor de servicios 1 para almacenamiento y para uso durante el proceso de pre registro y de registro, respectivamente, de un primer servicio en la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1.

En el paso (12) de la figura 1 datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida asignado son enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario. En particular, datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario son enviados a la aplicación software protegida de dispositivo móvil no personalizada en seguridad en el dispositivo móvil del usuario. Conforme a algunas implementaciones (en relación a la figura 2.g) [$ps_{1b\text{-}RPS43}$, $ro_{1b\text{-}RPS43}$, $ch_{1b\text{-}RPS43}$] son enviados en formato ofuscado a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1.

En el paso (13) de la figura 1 el dispositivo móvil del usuario recibe los datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones la habilitación de el al menos uno de los uno o más primeros dominios de código está asociada a uno o más parámetros de seguridad relativos al registro de personalización de seguridad de ciclo de vida (ej. $ps_{1b\text{-}RPS43}$ relativo al registro de personalización de seguridad de ciclo de vida RPS43), que son diferentes que los correspondientes del registro de personalización de seguridad (ej. $ps_{1b\text{-}RPS21}$, $ps_{1b\text{-}RPS31}$, $ps_{1b\text{-}RPS41}$, …, $ps_{1b\text{-}RPSi1}$, …. $ps_{1b\text{-}RPSn1}$ en relación a RPS-I).

Conforme a algunas implementaciones (en relación a la figura 2.g) el dispositivo móvil del usuario 1 recibe en formato ofuscado (la ofuscación usando un método que usa un parámetro de seguridad que está embebido en una función de DC1 y al menos parte de $IDD_{USUARIO1}$) el valor de dato para almacenamiento en la parte de la aplicación software protegida de dispositivo móvil asociada a $ps_{DCs\text{-}asignación}$, dicho valor haciendo que la aplicación software protegida de dispositivo móvil use DC4/1, DC4/2 y DC1 durante su ejecución. En estas implementaciones el dispositivo móvil del usuario 1 también recibe [$ps_{1b\text{-}RPS43}$, $ro_{1b\text{-}RPS43}$, $ch_{1b\text{-}RPS43}$] en formato ofuscado desde el proveedor de servicios de personalización y estos son almacenados en la parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a DC4/1 (como se ilustra en la figura 2.h). Los datos de personalización de seguridad [$ps_{1b\text{-}RPS43}$, $ro_{1b\text{-}RPS43}$, $ch_{1b\text{-}RPS43}$] recibidos y almacenados habilitan el primer dominio de código DC4/1 para operación regular, la ofuscación de dichos datos siendo relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en el segundo dominio de código DC1 y que son requeridos para habilitar el primer dominio de código DC4/1 para operación regular, como se ha descrito en relación a la figura 2.d.

Ventajosamente, después de que la personalización de seguridad anterior haya sido realizada, el referido al menos uno de los uno o más primeros dominios de código pueden ser usados para realizar regularmente las funciones asociadas de ciclo de vida de la aplicación.

Durante su ciclo de vida la aplicación software protegida de dispositivo móvil será capaz de des ofuscar $ps_{DCs\text{-}asignación}$ y de determinar que DC4/1, DC4/2 y DC1 deben ser usados durante su ejecución. También, la aplicación software protegida de dispositivo móvil será capaz de des ofuscar [$ps_{1b\text{-}RPS43}$, $ro_{1b\text{-}RPS43}$, $ch_{1b\text{-}RPS43}$] usando el algoritmo de ofuscación y la clave de ofuscación que protege datos de personalización de seguridad DC4/1, como ya se ha ilustrado en relación a la figura 2.g (x = 4). Más en detalle:

- Para solicitar el pre registro de un primer servicio, una o más partes de [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil, y un cálculo basado en las una o más partes des ofuscadas de [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$] es enviado al proveedor de servicios 1 para verificación de que la solicitud es enviada desde el dispositivo apropiado y ha sido lanzada desde el dominio de código adecuado (DC4/1) con la correcta personalización de seguridad. Como se ha referido anteriormente, el proveedor de servicios 1 ha almacenado previamente las una o más partes de [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$] en relación al dispositivo móvil del usuario 1, para usarlas durante el proceso de verificación.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$sp_{1a\text{-}RS4}$ / $sp_{1b\text{-}RPS43}$] son usadas para proteger al menos parte de la parte de la base de datos de la aplicación asociada a DC4/1 y DC4/2 (y no asociada a personalización / asignación de seguridad de dominios de código). Cuando la aplicación software protegida de dispositivo móvil requiere del uso de datos almacenados en dicha al menos parte de la parte de la base de datos, las otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar los datos en la base de datos, para uso.

- Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS4}$ / $ps_{1b\text{-}RPS43}$] serán des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para calcular la clave de ofuscación para des ofuscar [$ps_{2b\text{-}RPS43}$], [$ch_{2b\text{-}RPS43}$] y [$ro_{2b\text{-}RPS43}$], cuando sea requerido.

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ch_{1a\text{-}RS4}$, $ch_{1b\text{-}RPS43}$] serán usados para verificar la integridad de las partes relativas del código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{1a\text{-}RS4}$, $ch_{1b\text{-}RPS43}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. Como se ha referido anteriormente, en estas implementaciones $ch_{1b\text{-}RPS43} = ch_{1b\text{-}RPS41}$;

  - Conforme a las implementaciones alternativas referidas anteriormente, $ch_{1b\text{-}RPS43} = ch_{1b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ ha sido establecido a un valor dado tal que una o más partes asociadas de la red de checksums [$ch_{1a\text{-}RS4}$ / $ch_{1b\text{-}RPS43}$] serán usadas para verificar la integridad de partes relativas del código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …) y de al menos partes relativas de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …);

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ro_{1a\text{-}RS4}$, $ro_{1b\text{-}RPS43}$] será usada para des ofuscar la parte relativa del código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …), la parte relativa de los [$ps_{1a\text{-}RS4}$, $ps_{3\text{-}RS4,}$ $ps_{4\text{-}RS4}$ …, $ps_{i\text{-}RS4}$] y la parte relativa de los [$ch_{1a\text{-}RS4}$, $ch_{3\text{-}RS4,}$ $ch_{4\text{-}RS4}$ …, $ch_{i\text{-}RS4}$] embebidos en el código de la aplicación de las funciones DC4/1($f1_{DC4/1}$, $f2_{DC4/1,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha parte referida del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{1a\text{-}RS4}$ / $ro_{1b\text{-}RPS43}$]. Como se ha referido anteriormente, en estas implementaciones $ro_{1b\text{-}RPS43} = ro_{1b\text{-}rps41}$;

  - Conforme a las implementaciones alternativas referidas anteriormente $ro_{1b\text{-}RPS43} = or_{1b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{1a\text{-}RS4}$ / $ro_{1b\text{-}RPS43}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos de la réplica de la función $fi_{DC4/1}$ en DC4/1 que está asociada al valor dado del parámetro cuando la aplicación software protegida de dispositivo móvil requiere el uso de dicha parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos.

En referencia nuevamente a la figura 1, conforme a algunas implementaciones diferentes grupos de uno o más primeros dominios de código no-habilitados son personalizados en términos de seguridad en diferentes instantes de tiempo. Esta aproximación incrementa la seguridad de la aplicación software protegida de dispositivo móvil.

En las implementaciones descritas en las figuras 2.a a 2.l, DCx/2 son otros primeros dominios de código. Los pasos (14a) a (14e) descritos a continuación son relativos a la aplicación software protegida de dispositivo móvil instalada en el dispositivo móvil del usuario 1, el registro de personalización de seguridad de ciclo de vida asignado es RPS43 y $ps_{DCs\text{-}asignación}$ tiene un valor de dato asignado asociado a DC4/1 y DC4/2, por lo que en este contexto DC4/2 es el otro primer dominio de código.

También, por simplicidad, en el contexto de las figuras 2.a a 2.l, los pasos (15a) a (15e) y los pasos (16a) a (16e) no tienen lugar.

Tal y como ya se ha descrito en la figura 1, el paso (14a) representa una solicitud sucesiva para una personalización de seguridad de al menos otro uno o más primeros dominios de código, enviada desde el

dispositivo móvil del usuario al proveedor de servicios de personalización (en el contexto actual: una personalización de seguridad de DC4/2 enviada desde el dispositivo móvil del usuario 1).

En estas implementaciones, cada solicitud de dispositivo móvil de usuario es lanzada por uno o más dispositivos de procesamiento usando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular (en el contexto actual: eso es código ejecutable perteneciente a DC4/1, la solicitud lanzada desde el dispositivo móvil del usuario 1).

En el paso (14a) de la figura 1 una solicitud sucesiva es enviada desde el dispositivo móvil del usuario 1 al proveedor de servicios de personalización y en el paso (14b) el proveedor de servicios de personalización recibe la solicitud sucesiva desde el dispositivo móvil del usuario 1, y uno o más dispositivos de procesamiento del proveedor de servicios de personalización pueden obtener en el paso (14c) datos de personalización de seguridad ([$ps_{2b\text{-}RPS43}$, $ro_{2b\text{-}RPS43}$, $ch_{2b\text{-}RPS43}$]) desde el registro de personalización de seguridad de ciclo de vida previamente asignado al dispositivo móvil del usuario (desde RPS43). Conforme a algunas implementaciones los datos de personalización de seguridad han sido previamente obtenidos del registro de personalización de seguridad: esto puede ser realizado ej. en el paso (10), donde como se ha descrito anteriormente ([$ps_{2b\text{-}RPS43}$, $ro_{2b\text{-}RPS43}$, $ch_{2b\text{-}RPS43}$] han sido almacenados en formato ofuscado en la base de datos asociada a aplicaciones software protegidas de dispositivo móvil, en relación al dispositivo móvil del usuario 1, la aplicación software protegida de dispositivo móvil y el proceso de personalización de seguridad.

En el paso (14d) de la figura 1 los datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida RPS43 previamente asignado al dispositivo móvil del usuario 1 son enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario 1. En particular, datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida (RPS43) son enviados a la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad. Conforme a algunas implementaciones (en relación a la figura 2.g) [$ps_{2b\text{-}RPS43}$, $ro_{2b\text{-}RPS43}$, $ch_{2b\text{-}RPS43}$] son enviados en formato ofuscado a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1.

En el paso (14e) de la figura 1 el dispositivo móvil del usuario 1 recibe desde el proveedor de servicios de personalización los datos de personalización de seguridad ([$ps_{2b\text{-}RPS43}$, $ro_{2b\text{-}RPS43}$, $ch_{2b\text{-}RPS43}$] en formato ofuscado) asociados al registro de personalización de seguridad de ciclo de vida (RPS43) relativo al dispositivo móvil del usuario 1 en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos son almacenados en la parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a DC4/2 (como se ilustra en la figura 2.i), los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código (DC4/2) que está asociado a la solicitud particular.

Conforme a algunas implementaciones, al menos uno del otro uno o más primeros dominios de código (DC4/2) está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código (DC4/1) a través de la personalización de seguridad ([$ps_{2b\text{-}RPS43}$, $ro_{2b\text{-}RPS43}$, $ch_{2b\text{-}RPS43}$]), dicha personalización relativa a parámetros de seguridad (al menos parte de [$ps_{1a\text{-}RS4}$, $ps_{1b\text{-}RPS43}$]) y/o reglas de ofuscación (al menos parte de [$ro_{1a\text{-}RS4}$, $ro_{1b\text{-}RPS43}$]) y/o datos de checksums de código (al menos parte de [$ch_{1a\text{-}RS4}$, $ch_{1b\text{-}RPS43}$]) que están al menos parcialmente disponibles en los uno o más primeros dominios de código (DC4/1) y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones, al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario y están disponibles en una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a uno o más primeros dominios de código que han sido previamente habilitados para operación regular ([$ps_{1b\text{-}RPS43}$]) y/o [$ro_{1b\text{-}RPS43}$]) y/o [$ch_{1b\text{-}RPS43}$] están disponibles en una parte de la base de datos de la aplicación que está asociada a DC4/1).

Ventajosamente, una vez que la personalización de seguridad anterior ha sido realizada, el referido al menos otro uno o más primeros dominios de código puede ser usado para realizar regularmente las funciones asociadas de ciclo de vida de la aplicación.

Durante su ciclo de vida la aplicación software protegida de dispositivo móvil será capaz de des ofuscar [$ps_{2b\text{-}RPS43}$, $ro_{2b\text{-}RPS43}$, $ch_{2b\text{-}RPS43}$] usando el algoritmo de ofuscación y la clave de ofuscación que protege datos de personalización de seguridad DC4/2, como ya se ha ilustrado en relación a la figura 2.g (x = 4). Más en detalle:

- Para solicitar el registro del primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC4/2 tras un pre registro previo con éxito del primer servicio), una o más partes de [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil, y un cálculo basado en las des ofuscadas una o más partes de [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] es enviado al proveedor de servicios 1 para verificación de que la solicitud es enviada desde el dispositivo apropiado y ha sido lanzada desde el dominio de código adecuado (DC4/2) con la personalización de seguridad adecuada. Como se ha referido anteriormente, el proveedor de servicios 1 ha almacenado previamente las una o más partes de [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] en relación al dispositivo móvil del usuario 1, para usarlas durante el proceso de verificación.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] son usadas para proteger ciertos datos sensibles no estructurados antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1. Conforme a algunas implementaciones cuando la aplicación software protegida de dispositivo móvil requiere el uso de al menos parte de los datos sensibles no estructurados, las otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar los al menos parte de los datos sensibles no estructurados almacenados, para uso.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] son usadas para ofuscar ciertos datos sensibles, en el contexto de la ejecución de algunas instrucciones de código DC4/2, para evitar que sean expuestos en claro en una o más memorias de trabajo del dispositivo móvil del usuario 1. Cuando, durante la ejecución de ciertas instrucciones de código DC4/2, uno o más dispositivos de procesamiento en el dispositivo móvil del usuario 1 requieren usar los datos sensibles ofuscados previamente almacenados en las una o más memorias de trabajo, estos utilizan las otras una o más partes de [$ps_{2a\text{-}RS4}$ / $ps_{2b\text{-}RPS43}$] (y la regla de ofuscación referida anteriormente en relación a la figura 2.b) para obtener los datos adecuados para el relativo cálculo/proceso.

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ch_{2a\text{-}RS4}$, $ch_{2b\text{-}RPS43}$] será usado para verificar la integridad de las partes relativas del código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{2a\text{-}RS4}$, $ch_{2b\text{-}RPS43}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. Como se ha referido anteriormente, en estas implementaciones $ch_{2b\text{-}RPS43} = ch_{2b\text{-}RPS41}$;

  - Conforme a las implementaciones alternativas referidas anteriormente, $ch_{2b\text{-}RPS43} = ch_{2b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ ha sido establecido a un valor dado tal que una o más partes asociadas de la red de checksums [$ch_{2a\text{-}RS4}$ / $ch_{2b\text{-}RPS43}$] serán usadas para verificar la integridad de partes relativas del código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …) y de al menos partes relativas de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …);

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ro_{2a\text{-}RS4}$, $ro_{2b\text{-}RPS43}$] será usada para des ofuscar la parte relativa del código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …), la parte relativa de los [$ps_{2a\text{-}RS4}$, $ps_{(i+1)\text{-}RS4,}$ $ps_{(i+2)\text{-}RS4}$ …, $ps_{q\text{-}RS4}$] y la parte relativa de los [$ch_{2a\text{-}RS4}$, $ch_{(i+1)\text{-}RS4,}$ $ch_{(i+2)\text{-}RS4}$ …, $ch_{q\text{-}RS4}$] embebidos en el código de la aplicación de las funciones DC4/2($f1_{DC4/2}$, $f2_{DC4/2,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha referida parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{2a\text{-}RS4}$ / $ro_{2b\text{-}RPS43}$]. Como se ha referido anteriormente, en estas implementaciones $ro_{2b\text{-}RPS43} = ro_{2b\text{-}RPS41}$;

  - Conforme a las implementaciones alternativas referidas anteriormente $ro_{2b\text{-}RPS43} = ro_{2b\text{-}RPS41}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{2a\text{-}RS4}$ / $ro_{2b\text{-}RPS43}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos de la réplica de la función $fi_{DC4/2}$ en DC4/2 que está asociada al valor dado del parámetro cuando la aplicación software protegida de dispositivo móvil requiere el uso de dicha parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas.

En un ejemplo particular los procesos incluyendo hasta el paso 13 ya han sido realizados tal que la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1 está en un estado parcialmente personalizado de seguridad. Como se ha descrito anteriormente, en el paso (14a) una solicitud sucesiva es enviada desde el dispositivo móvil del usuario 1 y recibida en el paso (14b) por el proveedor de servicios de personalización. En este ejemplo, al inicio del paso (14c), uno o más dispositivos de procesamiento del proveedor de servicios de personalización verifican si la solicitud ha sido recibida (paso 14b) más tarde que un periodo predefinido de tiempo después de que datos de personalización de seguridad fueran enviados a la aplicación software protegida de dispositivo móvil en el paso (12).

Si la solicitud ha sido recibida más tarde que dicho periodo predefinido de tiempo, entonces la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad asociada al dispositivo móvil del usuario 1 expira en el sistema del proveedor de servicios de personalización. Conforme a algunas implementaciones, el proveedor de servicios de personalización notifica (no ilustrado en la figura 1) al proveedor de servicios 1 acerca del estado de expiración de la aplicación software protegida de dispositivo móvil asociada al dispositivo móvil del usuario 1. También, una notificación indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado es enviada al dispositivo móvil del usuario 1 y recibida en el dispositivo móvil del usuario 1.

Por tanto, conforme a algunas implementaciones uno o más dispositivos de procesamiento en el sistema del proveedor de servicios de personalización hacen una aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad expirar si una solicitud para una personalización de seguridad de al menos otro uno o más primeros dominios de código (ej. DC4/2) es recibida más tarde que un periodo de tiempo predefinido después de que datos de personalización de seguridad relativos a una solicitud previa para una personalización de seguridad de al menos uno (ej. DC4/1) u otro diferente uno de los uno o más primeros dominios de código fueran enviados a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada o parcialmente-personalizada. Esta aproximación incrementa adicionalmente la seguridad de la aplicación software protegida de dispositivo móvil.

También, conforme a algunas implementaciones, una notificación desde el proveedor de servicios de personalización indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado es enviada al dispositivo móvil del usuario 1 y recibida en el dispositivo móvil del usuario 1.

Conforme a algunas implementaciones:

- $[ps_{1b\text{-}RPS43}, ro_{1b\text{-}RPS43}, ch_{1b\text{-}RPS43}]$ en formato ofuscado son enviadas a (paso (12)) y almacenadas en (paso (13) la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 1. Los datos de personalización de seguridad $[ps_{1b\text{-}RPS43}, ro_{1b\text{-}RPS43}, ch_{1b\text{-}RPS43}]$ recibidos y almacenados habilitan el primer dominio de código CD4/1 para operación regular.

- Una o más partes de $[ps_{1a\text{-}RS4}, ps_{1b\text{-}RPS43}]$ serán posteriormente usadas para validar que una solicitud para pre registrar un primer servicio, asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 1, y ha sido lanzada desde DC4/1 con la personalización de seguridad adecuada. En un ejemplo particular el usuario 1 obtiene un código de activación y este es enviado en el contexto del proceso de pre registro del primer servicio, desde el dispositivo móvil del usuario 1 al proveedor de servicios de personalización, para validación. En un ejemplo particular los pasos (14a) a (14e) son también realizados en el contexto del proceso de pre registro del primer servicio (ej. tras una validación con éxito del código de activación referido en el ejemplo previo), por lo que $[ps_{2b\text{-}RPS43}, ro_{2b\text{-}RPS43}, ch_{2b\text{-}RPS43}]$ serán recibidos y almacenados en formato ofuscado en la parte de la base de datos de la aplicación asociada a DC4/2 antes de que el proceso de pre registro del primer servicio finalice.

- Una o más partes de $[ps_{2a\text{-}RS4}, ps_{2b\text{-}RPS43}]$ serán más tarde usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC4/2 tras un pre registro previo con éxito del primer servicio), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 1 y ha sido lanzada desde DC4/2 con la personalización de seguridad adecuada.

  En un ejemplo particular un PIN (Número de Identificación Personal) es seleccionado por el usuario 1 e insertado en el dispositivo móvil del usuario 1 durante el proceso de registrar dicho primer servicio en la aplicación software protegida de dispositivo móvil y datos enviados a y almacenados en la base de datos de la aplicación software protegida de dispositivo móvil durante el proceso de pre registro de dicho primer

servicio son usados para autenticar el registro del PIN seleccionado en el sistema del proveedor de servicios 1 (ej. dichos datos pueden permitir calcular una credencial dinámica basada-en-PIN que puede ser autenticada por el proveedor de servicios de personalización, así asegurando que el cálculo ha sido realizado desde el dispositivo móvil del usuario 1 y ej. por funciones en DC4/2, con la personalización de seguridad adecuada aplicada).

Si las validaciones tienen éxito el proceso de registro puede concluir con éxito (ej. enviando datos asociados al proceso de registro del primer servicio al dispositivo móvil del usuario 1).

Conforme a algunas implementaciones, adicionalmente a establecer un límite de tiempo entre los pasos (12) y (14b) para que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad expire, otro límite de tiempo asociado al total del proceso de pre registro y de registro del primer servicio en la aplicación software protegida de dispositivo móvil puede ser establecido, una vez que la aplicación software protegida de dispositivo móvil ya está en un estado de personalización parcial de seguridad. Ventajosamente, esos límites de tiempo pueden incrementar la seguridad del sistema.

La figura 2.g es también relativa a un escenario donde la aplicación software protegida de dispositivo móvil es instalada en el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$), y los pasos (8), (9) y (10) tienen lugar en relación a dicho dispositivo móvil del usuario 2. En el ejemplo ilustrado en la figura 2.g el registro de personalización de seguridad de ciclo de vida asignado por el módulo de personalización de seguridad al dispositivo móvil del usuario 2 es RPS32, que tal y como se ha referido anteriormente está asociado a DC3/1, DC3/2 y DC1. Todavía en el paso (10) la asignación del registro de personalización de seguridad de ciclo de vida RPS32 al dispositivo móvil del usuario 2 y a la aplicación software protegida de dispositivo móvil es almacenada en la base de datos asociada a aplicaciones software de dispositivo móvil.

En más detalle, conforme a algunas implementaciones el módulo de personalización de seguridad puede realizar las siguientes asignaciones y preparación de datos en el paso (10) (algunos de los procesos de preparación de datos pueden también ser realizados en una fase posterior, antes de enviar los datos a la aplicación software protegida de dispositivo móvil), in relación al dispositivo móvil del usuario 2 y a la personalización de seguridad:

- Asignación de RPS32 en el contexto del proceso de personalización de seguridad en curso, asociado a DC3/1, DC3/2 y CD1 y a $IDD_{USUARIO2}$;
- Asignar a $ps_{DCs\text{-}asignación}$ un valor de dato asociado a DC3/1 y DC3/2 tal que, una vez personalizado en términos de seguridad, la aplicación software protegida de dispositivo móvil usará DC3/1, DC3/2 y DC1 durante su ejecución. En estas implementaciones el valor de dato es ofuscado usando un método que usa un parámetro de seguridad que está embebido en una función DC1 y al menos parte de $IDD_{USUARIO2}$.
- Ofuscación de [$ps_{1b\text{-}RPS32}$, $ro_{1b\text{-}RPS32}$, $ch_{1b\text{-}RPS32}$] usando un algoritmo de ofuscación y la clave de ofuscación para proteger datos de personalización de seguridad DC3/1, como se ilustra en la figura 2.g (en este proceso de personalización de seguridad x = 3). En estas implementaciones:
  - los primeros 10 dígitos de $IDD_{USUARIO2}$ son parte de la clave de ofuscación;
  - [$ps_{1a\text{-}RS3}$, $ps_{1b\text{-}RPS32}$] se convierten en las dos partes del mismo parámetro de seguridad:
    - Una o más partes de [$ps_{1a\text{-}RS3}$, $ps_{1b\text{-}RPS32}$] serán usadas para validar que una solicitud para pre registrar un primer servicio, asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC3/1 con la personalización de seguridad adecuada;
    - Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] serán usadas para proteger datos en ciertas partes de la base de datos de la aplicación software protegida de dispositivo móvil (en este contexto, ciertas partes asociadas a DC3/1 y DC3/2). En estas implementaciones, dichas otras una o más partes del parámetro de seguridad son usadas para proteger al menos parte de la parte de la base de datos de la aplicación que no está asociada a personalización / asignación de seguridad de dominios de código.

      Cuando la aplicación software protegida de dispositivo móvil recibe datos para almacenamiento en la al menos parte de la parte de la base de datos que no está asociada a

personalización / asignación de seguridad de dominios de código, esos son cifrados usando las referidas otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$], antes de ser almacenados en la correspondiente al menos parte de la parte de la base de datos de la aplicación.

- Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] son asignadas como el parámetro de seguridad que es parte de la clave de ofuscación usada para ofuscar [$ps_{2b\text{-}RPS32}$], [$ch_{2b\text{-}RPS32}$] y [$ro_{2b\text{-}RPS32}$].

○ [$ch_{1a\text{-}RS3}$, $ch_{1b\text{-}RPS32}$] se convierten en las dos partes de la misma red de checksums, que será usada para verificar la integridad de partes del código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …).

- En estas implementaciones $ch_{1b\text{-}RPS32} = ch_{1b\text{-}RPS31}$;
- Conforme a algunas implementaciones alternativas $ch_{1b\text{-}RPS32} = ch_{1b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la red de checksums [$ch_{1a\text{-}RS3}$ / $ch_{1b\text{-}RPS32}$] serán usadas para verificar la integridad de partes del código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …);

○ [$ro_{1a\text{-}RS3}$, $ro_{1b\text{-}RPS32}$] se convierten en las dos partes de la misma regla de ofuscación, que es usada para ofuscar parte del código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …) junto con parte de los [$ps_{1a\text{-}RS3}$, $ps_{3\text{-}RS3,}$ $ps_{4\text{-}RS3}$ …, $ps_{h\text{-}RS3}$] y parte de los [$ch_{1a\text{-}RS3}$, $ch_{3\text{-}RS3,}$ $ch_{4\text{-}RS3}$ …, $ch_{h\text{-}RS3}$] embebidos en el código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …).

- En estas implementaciones $ro_{1b\text{-}RPS32} = ro_{1b\text{-}RPS31}$;
- Conforme a algunas implementaciones alternativas $ro_{1b\text{-}RPS32} = ro_{1b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{1a\text{-}RS3}$ / $ro_{1b\text{-}RPS32}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la réplica de la función $fi_{DC3/1}$ en DC3/1 que está asociada al valor dado del parámetro.

- Ofuscación de [$ps_{2b\text{-}RPS32}$, $ro_{2b\text{-}RPS32}$, $ch_{2b\text{-}RPS32}$] usando un algoritmo de ofuscación y la clave de ofuscación para proteger datos de personalización de seguridad DC3/2, como se ilustra en la figura 2.g (en este proceso de personalización de seguridad x = 3). En estas implementaciones:

  ○ El parámetro de seguridad que es parte de la clave de ofuscación está constituido por al menos parte de [$ps_{1a\text{-}RS3}$] y al menos parte de [$ps_{1b\text{-}RPS32}$]. Los primeros 10 dígitos de $IDD_{USUARIO2}$ son también parte de la clave de ofuscación;

  ○ [$ps_{2a\text{-}RS3}$, $ps_{2b\text{-}RPS32}$] se convierten en las dos partes del mismo parámetro de seguridad:

  - Una o más partes de [$ps_{2a\text{-}RS3}$, $ps_{2b\text{-}RPS32}$] serán usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC3/2 tras un pre registro previo con éxito del primer servicio), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC3/2 con la personalización de seguridad adecuada;
  - Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] serán usadas para proteger ciertos datos sensibles no estructurados antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 (ej. para proteger claves/datos sensibles necesarios para que la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 calcule credenciales dinámicas asociadas a servicios provistos por el proveedor de servicios 1; ej. protección de claves de sesión), cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DC3/1 y DC3/2.

- Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] serán usadas por la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 para ofuscar ciertos datos sensibles, en el contexto de la ejecución de algunas instrucciones de código DC3/2, para evitar que sean expuestas en claro en una o más memorias de trabajo del dispositivo móvil, cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DC3/1 y DC3/2.

○ [$ch_{2a\text{-}RS3}$, $ch_{2b\text{-}RPS32}$] se convierten en las dos partes de la misma red de checksums, que será usada para verificar la integridad de partes del código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de funciones CD3/2($f1_{CD3/2}$, $f2_{CD3/2,}$ …).

- En estas implementaciones $ch_{2b\text{-}RPS32} = ch_{2b\text{-}RPS31}$;

- Conforme a algunas implementaciones alternativas $ch_{2b\text{-}RPS32} = ch_{2b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la red de checksums [$ch_{2a\text{-}RS3}$ / $ch_{2b\text{-}RPS32}$] serán usadas para verificar la integridad de partes del código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …);

○ [$ro_{2a\text{-}RS3}$, $ro_{2b\text{-}RPS32}$] se convierten en las dos partes de la misma regla de ofuscación, que son usadas para ofuscar parte del código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …) junto con parte de los [$ps_{2a\text{-}RS3}$, $ps_{(h+1)\text{-}RS3,}$ $ps_{(h+2)\text{-}RS3}$ …, $ps_{p\text{-}RS3}$] y parte de los [$ch_{2a\text{-}RS3}$, $ch_{(h+1)\text{-}RS3,}$ $ch_{(h+2)\text{-}RS3}$ …, $ch_{p\text{-}RS3}$] embebidos en el código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …).

- En estas implementaciones $ro_{2b\text{-}RPS32} = ro_{2b\text{-}RPS31}$;

- Conforme a algunas implementaciones alternativas $ro_{2b\text{-}RPS32} = ro_{2b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{2a\text{-}RS3}$ / $ro_{2b\text{-}RPS32}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la réplica de la función $fi_{DC3/2}$ en DC3/2 que está asociada al valor dado del parámetro.

Estas asignaciones y datos preparados son almacenados en la base de datos asociada a aplicaciones software de dispositivo móvil, en relación al dispositivo móvil del usuario 2, la aplicación software protegida de dispositivo móvil y el proceso de personalización de seguridad.

En el paso (11) de la figura 1 al menos parte del registro de personalización de seguridad de ciclo de vida asignado, y la asociación al dispositivo móvil del usuario y a la aplicación software protegida de dispositivo móvil es enviada al proveedor de servicios correspondiente tal que pueda usar al menor parte de ello en el contexto de ciertos procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil. Conforme a algunas implementaciones (en relación a la figura 2.g) al menos parte de las asignaciones y datos asociados al dispositivo móvil del usuario 2 y a la personalización de seguridad de la aplicación software protegida de dispositivo móvil son enviados al proveedor de servicios 1 para almacenamiento y/o para uso de al menos parte de ello en el contexto de ciertos procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil asociada al dispositivo móvil del usuario 2. En un ejemplo particular:

- Las una o más partes de [$ps_{1a\text{-}RS3}$, $ps_{1b\text{-}RPS32}$] que serán usadas para validar que una solicitud para pre registrar un primer servicio, asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC3/1 con la personalización de seguridad adecuada y;

- Las una o más partes de [$ps_{2a\text{-}RS3}$, $ps_{2b\text{-}RPS32}$] que serán usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC3/2 tras un pre registro previo con éxito del primer servicio), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC3/2 con la personalización de seguridad adecuada;

son enviadas al proveedor de servicios 1 para almacenamiento y para uso durante el proceso de pre registro y de registro, respectivamente, de un primer servicio en la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2.

En el paso (12) de la figura 1 datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida asignado son enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario. En particular, datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario son enviados a la aplicación software protegida de dispositivo móvil no personalizada en seguridad en el dispositivo móvil del usuario. Conforme a algunas implementaciones (en relación a la figura 2.g) [$ps_{1b\text{-}RPS32}$, $ro_{1b\text{-}RPS32}$, $ch_{1b\text{-}RPS32}$] son enviados en formato ofuscado a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2.

En el paso (13) de la figura 1 el dispositivo móvil del usuario recibe los datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones la habilitación de el al menos uno de los uno o más primeros dominios de código está asociada a uno o más parámetros de seguridad relativos al registro de personalización de seguridad de ciclo de vida (ej. $ps_{1b\text{-}RPS32}$ relativo al registro de personalización de seguridad de ciclo de vida RPS32), que son diferentes que los correspondientes del registro de personalización de seguridad (ej. $ps_{1b\text{-}RPS21}$, $ps_{1b\text{-}RPS31}$, $ps_{1b\text{-}RPS41}$, …, $ps_{1b\text{-}RPSi1}$, …. $ps_{1b\text{-}RPSn1}$ en relación a RPS-I).

Conforme a algunas implementaciones (en relación a la figura 2.g) el dispositivo móvil del usuario 2 recibe en formato ofuscado (la ofuscación usando un método que usa un parámetro de seguridad que está embebido en una función de DC1 y al menos parte de $IDD_{USUARIO2}$) el valor de dato para almacenamiento en la parte de la aplicación software protegida de dispositivo móvil asociada a $ps_{DCs\text{-}asignación}$, dicho valor haciendo que la aplicación software protegida de dispositivo móvil use DC3/1, DC3/2 y DC1 durante su ejecución. En estas implementaciones el dispositivo móvil del usuario 2 también recibe [$ps_{1b\text{-}RPS32}$, $ro_{1b\text{-}RPS32}$, $ch_{1b\text{-}RPS32}$] en formato ofuscado desde el proveedor de servicios de personalización y estos son almacenados en la parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a DC3/1 (como se ilustra en la figura 2.j). Los datos de personalización de seguridad [$ps_{1b\text{-}RPS32}$, $ro_{1b\text{-}RPS32}$, $ch_{1b\text{-}RPS32}$] recibidos y almacenados habilitan el primer dominio de código DC3/1 para operación regular, la ofuscación de dichos datos siendo relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en el segundo dominio de código DC1 y que son requeridos para habilitar el primer dominio de código DC3/1 para operación regular, como se ha descrito en relación a la figura 2.d.

Ventajosamente, después de que la personalización de seguridad anterior haya sido realizada, el referido al menos uno de los uno o más primeros dominios de código pueden ser usados para realizar regularmente las funciones asociadas de ciclo de vida de la aplicación.

Durante su ciclo de vida la aplicación software protegida de dispositivo móvil será capaz de des ofuscar $ps_{DCs\text{-}asignación}$ y de determinar que DC3/1, DC3/2 y DC1 deben ser usados durante su ejecución. También, la aplicación software protegida de dispositivo móvil será capaz de des ofuscar [$ps_{1b\text{-}RPS32}$, $ro_{1b\text{-}RPS32}$, $ch_{1b\text{-}RPS32}$] usando el algoritmo de ofuscación y la clave de ofuscación que protege datos de personalización de seguridad DC3/1, como ya se ha ilustrado en relación a la figura 2.g (x = 3). Más en detalle:

- Para solicitar el pre registro de un primer servicio, una o más partes de [$ps_{1a\text{-}RS3}$ / $sp_{1b\text{-}RPS32}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil, y un cálculo basado en las una o más partes des ofuscadas de [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] es enviado al proveedor de servicios 1 para verificación de que la solicitud es enviada desde el dispositivo apropiado y ha sido lanzada desde el dominio de código adecuado (DC3/1) con la correcta personalización de seguridad. Como se ha referido anteriormente, el proveedor de servicios 1 ha almacenado previamente las una o más partes de [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] en relación al dispositivo móvil del usuario 2, para usarlas durante el proceso de verificación.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] son usadas para proteger al menos parte de la parte de la base de datos de la aplicación asociada a DC3/1 y DC3/2 (y no asociada a personalización / asignación de seguridad de dominios de código).

Cuando la aplicación software protegida de dispositivo móvil requiere del uso de datos almacenados en dicha al menos parte de la parte de la base de datos, las otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar los datos en la base de datos, para uso.

- Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] serán des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para calcular la clave de ofuscación para des ofuscar [$ps_{2b\text{-}RPS32}$], [$ch_{2b\text{-}RPS32}$] y [$ro_{2b\text{-}RPS32}$], cuando sea requerido.

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ch_{1a\text{-}RS3}$, $ch_{1b\text{-}RPS32}$] serán usados para verificar la integridad de las partes relativas del código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{1a\text{-}RS3}$, $ch_{1b\text{-}RPS32}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. Como se ha referido anteriormente, en estas implementaciones $ch_{1b\text{-}RPS32} = ch_{1b\text{-}RPS31}$;

  - Conforme a las implementaciones alternativas referidas anteriormente, $ch_{1b\text{-}RPS32} = ch_{1b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ ha sido establecido a un valor dado tal que una o más partes asociadas de la red de checksums [$ch_{1a\text{-}RS3}$ / $ch_{1b\text{-}RPS32}$] serán usadas para verificar la integridad de partes relativas del código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …) y de al menos partes relativas de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …);

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ro_{1a\text{-}RS3}$, $ro_{1b\text{-}RPS32}$] será usada para des ofuscar la parte relativa del código de la aplicación de las funciones DC3/1($f1_{DC3/1}$, $f2_{DC3/1,}$ …), la parte relativa de los [$ps_{1a\text{-}RS3}$, $ps_{3\text{-}RS3,}$ $ps_{4\text{-}RS3}$ …, $ps_{h\text{-}RS3}$] y la parte relativa de los [$ch_{1a\text{-}RS3}$, $ch_{3\text{-}RS3,}$ $ch_{4\text{-}RS3}$ …, $ch_{h\text{-}RS3}$] embebidos en el código de la aplicación de funciones CD3/1($f1_{CD3/1}$, $f2_{CD3/1,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha parte referida del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{1a\text{-}RS3}$ / $ro_{1b\text{-}RPS32}$]. Como se ha referido anteriormente, en estas implementaciones $ro_{1b\text{-}RPS32} = ro_{1b\text{-}RPS31}$;

  - Conforme a las implementaciones alternativas referidas anteriormente $ro_{1b\text{-}RPS32} = ro_{1b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{1a\text{-}RS3}$ / $ro_{1b\text{-}RPS32}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos de la réplica de la función $fi_{DC3/1}$ en DC3/1 que está asociada al valor dado del parámetro cuando la aplicación software protegida de dispositivo móvil requiere el uso de dicha parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos.

En referencia nuevamente a la figura 1, conforme a algunas implementaciones diferentes grupos de uno o más primeros dominios de código no-habilitados son personalizados en términos de seguridad en diferentes instantes de tiempo. Esta aproximación incrementa la seguridad de la aplicación software protegida de dispositivo móvil.

En las implementaciones descritas en las figuras 2.a a 2.l, DCx/2 son otros primeros dominios de código. Los pasos (14a) a (14e) descritos a continuación son relativos a la aplicación software protegida de dispositivo móvil instalada en el dispositivo móvil del usuario 2, el registro de personalización de seguridad de ciclo de vida asignado es RPS32 y $ps_{DCs\text{-}asignación}$ tiene un valor de dato asignado asociado a DC3/1 y DC3/2, por lo que en este contexto DC3/2 es el otro primer dominio de código.

También, por simplicidad, en el contexto de las figuras 2.a a 2.l, los pasos (15a) a (15e) y los pasos (16a) a (16e) no tienen lugar.

Tal y como ya se ha descrito en la figura 1, el paso (14a) representa una solicitud sucesiva para una personalización de seguridad de al menos otro uno o más primeros dominios de código, enviada desde el dispositivo móvil del usuario al proveedor de servicios de personalización (en el contexto actual: una personalización de seguridad de DC3/2 enviada desde el dispositivo móvil del usuario 2).

En estas implementaciones, cada solicitud de dispositivo móvil de usuario es lanzada por uno o más dispositivos de procesamiento usando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular (en el contexto actual: eso es código ejecutable perteneciente a DC3/1, la solicitud lanzada desde el dispositivo móvil del usuario 2).

En el paso (14a) de la figura 1 una solicitud sucesiva es enviada desde el dispositivo móvil del usuario 2 al proveedor de servicios de personalización y en el paso (14b) el proveedor de servicios de personalización recibe la solicitud sucesiva desde el dispositivo móvil del usuario 2, y uno o más dispositivos de procesamiento del proveedor de servicios de personalización pueden obtener en el paso (14c) datos de personalización de seguridad ([$ps_{2b\text{-}RPS32}$, $ro_{2b\text{-}RPS32}$, $ch_{2b\text{-}RPS32}$]) desde el registro de personalización de seguridad de ciclo de vida previamente asignado al dispositivo móvil del usuario (desde RPS32). Conforme a algunas implementaciones los datos de personalización de seguridad han sido previamente obtenidos del registro de personalización de seguridad: esto puede ser realizado ej. en el paso (10), donde como se ha descrito anteriormente [$ps_{2b\text{-}RPS32}$, $ro_{2b\text{-}RPS32}$, $ch_{2b\text{-}RPS32}$] han sido almacenados en formato ofuscado en la base de datos asociada a aplicaciones software protegidas de dispositivo móvil, en relación al dispositivo móvil del usuario 2, la aplicación software protegida de dispositivo móvil y el proceso de personalización de seguridad.

En el paso (14d) de la figura 1 los datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida RPS32 previamente asignado al dispositivo móvil del usuario 2 son enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario 2. En particular, datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida (RPS32) son enviados a la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad. Conforme a algunas implementaciones (en relación a la figura 2.g) [$ps_{2b\text{-}RPS32}$, $ro_{2b\text{-}RPS32}$, $ch_{2b\text{-}RPS32}$] son enviados en formato ofuscado a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2.

En el paso (14e) de la figura 1 el dispositivo móvil del usuario 2 recibe desde el proveedor de servicios de personalización los datos de personalización de seguridad ([$ps_{2b\text{-}RPS32}$, $ro_{2b\text{-}RPS32}$, $ch_{2b\text{-}RPS32}$] en formato ofuscado) asociados al registro de personalización de seguridad de ciclo de vida (RPS32) relativo al dispositivo móvil del usuario 2 en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos son almacenados en la parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a DC3/2 (como se ilustra en la figura 2.j), los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código (DC3/2) que está asociado a la solicitud particular.

Conforme a algunas implementaciones, al menos uno del otro uno o más primeros dominios de código (DC3/2) está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código (DC3/1) a través de la personalización de seguridad ([$ps_{2b\text{-}RPS32}$, $ro_{2b\text{-}RPS32}$, $ch_{2b\text{-}RPS32}$]), dicha personalización relativa a parámetros de seguridad (al menos parte de [$ps_{1a\text{-}RS3}$, $ps_{1b\text{-}RPS32}$]) y/o reglas de ofuscación (al menos parte de [$ro_{1a\text{-}RS3}$, $ro_{1b\text{-}RPS32}$]) y/o datos de checksums de código (al menos parte de [$ch_{1a\text{-}RS3}$, $ch_{1b\text{-}RPS32}$]) que están al menos parcialmente disponibles en los uno o más primeros dominios de código (DC3/1) y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

Conforme a algunas implementaciones, al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario y están disponibles en una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a uno o más primeros dominios de código que han sido previamente habilitados para operación regular ([$ps_{1b\text{-}RPS32}$]) y/o [$ro_{1b\text{-}RPS32}$]) y/o [$ch_{1b\text{-}RPS32}$] están disponibles en una parte de la base de datos de la aplicación que está asociada a DC3/1).

Ventajosamente, una vez que la personalización de seguridad anterior ha sido realizada, el referido al menos otro uno o más primeros dominios de código puede ser usado para realizar regularmente las funciones asociadas de ciclo de vida de la aplicación.

Durante su ciclo de vida la aplicación software protegida de dispositivo móvil será capaz de des ofuscar [$ps_{2b\text{-}RPS32}$, $ro_{2b\text{-}RPS32}$, $ch_{2b\text{-}RPS32}$] usando el algoritmo de ofuscación y la clave de ofuscación que protege datos de personalización de seguridad DC3/2, como ya se ha ilustrado en relación a la figura 2.g (x = 3). Más en detalle:

- Para solicitar el registro del primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC3/2 tras un pre registro previo con éxito del primer servicio), una o más partes de [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}}$

$_{RPS32}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil, y un cálculo basado en las des ofuscadas una o más partes de [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] es enviado al proveedor de servicios 1 para verificación de que la solicitud es enviada desde el dispositivo apropiado y ha sido lanzada desde el dominio de código adecuado (DC3/2) con la personalización de seguridad adecuada. Como se ha referido anteriormente, el proveedor de servicios 1 ha almacenado previamente las una o más partes de [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] en relación al dispositivo móvil del usuario 2, para usarlas durante el proceso de verificación.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] son usadas para proteger ciertos datos sensibles no estructurados antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2. Conforme a algunas implementaciones cuando la aplicación software protegida de dispositivo móvil requiere el uso de al menos parte de los datos sensibles no estructurados, las otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar los al menos parte de los datos sensibles no estructurados almacenados, para uso.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] son usadas para ofuscar ciertos datos sensibles, en el contexto de la ejecución de algunas instrucciones de código DC3/2, para evitar que sean expuestos en claro en una o más memorias de trabajo del dispositivo móvil del usuario 2. Cuando, durante la ejecución de ciertas instrucciones de código DC3/2, uno o más dispositivos de procesamiento en el dispositivo móvil del usuario 2 requieren usar los datos sensibles ofuscados previamente almacenados en las una o más memorias de trabajo, estos utilizan las otras una o más partes de [$ps_{2a\text{-}RS3}$ / $ps_{2b\text{-}RPS32}$] (y la regla de ofuscación referida anteriormente en relación a la figura 2.b) para obtener los datos adecuados para el relativo cálculo/proceso.

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ch_{2a\text{-}RS3}$, $ch_{2b\text{-}RPS32}$] será usado para verificar la integridad de las partes relativas del código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{2a\text{-}RS3}$, $ch_{2b\text{-}RPS32}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. Como se ha referido anteriormente, en estas implementaciones $ch_{2b\text{-}RPS32} = ch_{2b\text{-}RPS31}$;

  - Conforme a las implementaciones alternativas referidas anteriormente, $ch_{2b\text{-}RPS32} = ch_{2b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ ha sido establecido a un valor dado tal que una o más partes asociadas de la red de checksums [$ch_{2a\text{-}RS3}$ / $ch_{2b\text{-}RPS32}$] serán usadas para verificar la integridad de partes relativas del código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …) y de al menos partes relativas de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …);

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ro_{2a\text{-}RS3}$, $ro_{2b\text{-}RPS32}$] será usada para des ofuscar la parte relativa del código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …), la parte relativa de los [$ps_{2a\text{-}RS3}$, $ps_{(h+1)\text{-}RS3,}$ $ps_{(h+2)\text{-}RS3}$ …, $ps_{p\text{-}RS3}$] y la parte relativa de los [$ch_{2a\text{-}RS3}$, $ch_{(h+1)\text{-}RS3,}$ $ch_{(h+2)\text{-}RS3}$ …, $ch_{p\text{-}RS3}$] embebidos en el código de la aplicación de las funciones DC3/2($f1_{DC3/2}$, $f2_{DC3/2,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha referida parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{2a\text{-}RS3}$ / $ro_{2b\text{-}RPS32}$]. Como se ha referido anteriormente, en estas implementaciones $ro_{2b\text{-}RPS32} = ro_{2b\text{-}RPS31}$;

  - Conforme a las implementaciones alternativas referidas anteriormente $ro_{2b\text{-}RPS32} = ro_{2b\text{-}RPS31}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{2a\text{-}RS3}$ / $ro_{2b\text{-}RPS32}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos de la réplica de la función $fi_{DC3/2}$ en DC3/2 que está asociada al valor dado del parámetro cuando la aplicación software protegida de dispositivo móvil requiere el uso de dicha parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas.

En un ejemplo particular los procesos incluyendo hasta el paso 13 ya han sido realizados tal que la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 está en un estado parcialmente personalizado de seguridad. Como se ha descrito anteriormente, en el paso (14a) una solicitud sucesiva es enviada desde el dispositivo móvil del usuario 2 y recibida en el paso (14b) por el proveedor de servicios de

personalización. En este ejemplo, al inicio del paso (14c), uno o más dispositivos de procesamiento del proveedor de servicios de personalización verifican si la solicitud ha sido recibida (paso 14b) más tarde que un periodo predefinido de tiempo después de que datos de personalización de seguridad fueran enviados a la aplicación software protegida de dispositivo móvil en el paso (12).

Si la solicitud ha sido recibida más tarde que dicho periodo predefinido de tiempo, entonces la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad asociada al dispositivo móvil del usuario 2 expira en el sistema del proveedor de servicios de personalización. Conforme a algunas implementaciones, el proveedor de servicios de personalización notifica (no ilustrado en la figura 1) al proveedor de servicios 1 acerca del estado de expiración de la aplicación software protegida de dispositivo móvil asociada al dispositivo móvil del usuario 2. También, una notificación indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado es enviada al dispositivo móvil del usuario 2 y recibida en el dispositivo móvil del usuario 2.

Por tanto, conforme a algunas implementaciones uno o más dispositivos de procesamiento en el sistema del proveedor de servicios de personalización hacen una aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad expirar si una solicitud para una personalización de seguridad de al menos otro uno o más primeros dominios de código (ej. DC3/2) es recibida más tarde que un periodo de tiempo predefinido después de que datos de personalización de seguridad relativos a una solicitud previa para una personalización de seguridad de al menos uno (ej. DC3/1) u otro diferente uno de los uno o más primeros dominios de código fueran enviados a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada o parcialmente-personalizada. Esta aproximación incrementa adicionalmente la seguridad de la aplicación software protegida de dispositivo móvil.

También, conforme a algunas implementaciones, una notificación desde el proveedor de servicios de personalización indicando que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad ha expirado es enviada al dispositivo móvil del usuario 2 y recibida en el dispositivo móvil del usuario 2.

Conforme a algunas implementaciones:

- $[ps_{1b\text{-}RPS32}, ro_{1b\text{-}RPS32}, ch_{1b\text{-}RPS32}]$ en formato ofuscado son enviadas a (paso (12)) y almacenadas en (paso (13) la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2. Los datos de personalización de seguridad $[ps_{1b\text{-}RPS32}, ro_{1b\text{-}RPS32}, ch_{1b\text{-}RPS32}]$ recibidos y almacenados habilitan el primer dominio de código CD3/1 para operación regular.

- Una o más partes de $[ps_{1a\text{-}RS3}, ps_{1b\text{-}RPS32}]$ serán posteriormente usadas para validar que una solicitud para pre registrar un primer servicio, asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2, y ha sido lanzada desde DC3/1 con la personalización de seguridad adecuada. En un ejemplo particular el usuario 2 obtiene un código de activación y este es enviado en el contexto del proceso de pre registro del primer servicio, desde el dispositivo móvil del usuario 2 al proveedor de servicios de personalización, para validación. En un ejemplo particular los pasos (14a) a (14e) son también realizados en el contexto del proceso de pre registro del primer servicio (ej. tras una validación con éxito del código de activación referido en el ejemplo previo), por lo que $[ps_{2b\text{-}RPS32}, ro_{2b\text{-}RPS32}, ch_{2b\text{-}RPS32}]$ serán recibidos y almacenados en formato ofuscado en la parte de la base de datos de la aplicación asociada a DC3/2 antes de que el proceso de pre registro del primer servicio finalice.

- Una o más partes de $[ps_{2a\text{-}RS3}, ps_{2b\text{-}RPS32}]$ serán más tarde usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC3/2 tras un pre registro previo con éxito del primer servicio), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 y ha sido lanzada desde DC3/2 con la personalización de seguridad adecuada.

  En un ejemplo particular un PIN (Número de Identificación Personal) es seleccionado por el usuario 2 e insertado en el dispositivo móvil del usuario 2 durante el proceso de registrar dicho primer servicio en la aplicación software protegida de dispositivo móvil y datos enviados a y almacenados en la base de datos de la aplicación software protegida de dispositivo móvil durante el proceso de pre registro de dicho primer servicio son usados para autenticar el registro del PIN seleccionado en el sistema del proveedor de servicios 1 (ej. dichos datos pueden permitir calcular una credencial dinámica basada-en-PIN que puede ser autenticada por el proveedor de servicios de personalización, así asegurando que el cálculo ha sido

realizado desde el dispositivo móvil del usuario 2 y ej. por funciones en DC3/2, con la personalización de seguridad adecuada aplicada).

Si las validaciones tienen éxito el proceso de registro puede concluir con éxito (ej. enviando datos asociados al proceso de registro del primer servicio al dispositivo móvil del usuario 2).

Conforme a algunas implementaciones, adicionalmente a establecer un límite de tiempo entre los pasos (12) y (14b) para que la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad expire, otro límite de tiempo asociado al total del proceso de pre registro y de registro del primer servicio en la aplicación software protegida de dispositivo móvil puede ser establecido, una vez que la aplicación software protegida de dispositivo móvil ya está en un estado de personalización parcial de seguridad. Ventajosamente, esos límites de tiempo pueden incrementar la seguridad del sistema.

En las implementaciones descritas en relación a la figura 2.g, el registro de personalización de seguridad de ciclo de vida asignado al dispositivo móvil del usuario 1 (RPS43) es diferente que el registro de personalización de seguridad de ciclo de vida asignado al dispositivo móvil del usuario 2 (RPS32); y estos son ambos diferentes que el registro de personalización de seguridad usado cuando se genera la aplicación software de dispositivo móvil personalizada en seguridad (RPS-I).

También, como se ha detallado extensamente en relación a la figura 2.g, conforme a algunas implementaciones los uno o más primeros/segundos dominios de código asociados en una o más memorias del proveedor de servicios de personalización a la aplicación software protegida de dispositivo móvil en un dispositivo móvil de un primer usuario (primeros dominios de código DC4/1 y DC4/2, asociados al dispositivo móvil del usuario 1) son diferentes que los uno o más primeros/segundos dominios de código asociados en una o más memorias del proveedor de servicios de personalización a la aplicación software protegida de dispositivo móvil en un dispositivo móvil de un segundo usuario (primeros dominios de código DC3/1 y DC3/2, asociados la dispositivo móvil del usuario 2).

Y, conforme a algunas implementaciones los uno o más primeros dominios de código habilitados a través de primeros datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un primer usuario (primeros dominios de código DC4/1 y DC4/2, asociados al dispositivo móvil del usuario 1) son diferentes que los uno o más primeros dominios de código habilitados a través de segundos datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un segundo usuario (primeros dominios de código CD3/1 y CD3/2, asociados al dispositivo móvil del usuario 2).

Como también se ha descrito anteriormente, conforme a algunas implementaciones los datos de personalización de seguridad recibidos en el dispositivo móvil de un primer usuario, los datos (ej. $[ps_{1b\text{-}RPS43}]$, $[ch_{1b\text{-}RPS43}]$, $[ro_{1b\text{-}RPS43}]$ y $[ps_{2b\text{-}RPS43}]$, $[ch_{2b\text{-}RPS43}]$, $[ro_{2b\text{-}RPS43}]$ almacenados en la base de datos de la aplicación en formato ofuscado) habilitando en la aplicación uno o más primeros dominios de código (DC4/1 y DC4/2) para operación regular y asociados a un primer registro de personalización de seguridad de ciclo de vida (RPS43) que incluye primeros parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código ($[ps_{1b\text{-}RPS43}]$, $[ch_{1b\text{-}RPS43}]$, $[ro_{1b\text{-}RPS43}]$ y $[ps_{2b\text{-}RPS43}]$, $[ch_{2b\text{-}RPS43}]$, $[ro_{2b\text{-}RPS43}]$), son diferentes que los datos de personalización de seguridad recibidos en el dispositivo móvil de un segundo usuario, los datos (ej. $[ps_{1b\text{-}RPS32}]$, $[ch_{1b\text{-}RPS32}]$, $[ro_{1b\text{-}RPS32}]$ y $[ps_{2b\text{-}RPS32}]$, $[ch_{2b\text{-}RPS32}]$, $[ro_{2b\text{-}RPS32}]$ almacenados en la base de datos de la aplicación en formato ofuscado) habilitando en la aplicación uno o más primeros dominios de código (DC3/1 y DC3/2) para operación regular y asociados a un segundo registro de personalización de seguridad de ciclo de vida (RPS32) que incluye segundos parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código ($[ps_{1b\text{-}RPS32}]$, $[ch_{1b\text{-}RPS32}]$, $[ro_{1b\text{-}RPS32}]$ y $[ps_{2b\text{-}RPS32}]$, $[ch_{2b\text{-}RPS32}]$, $[ro_{2b\text{-}RPS32}]$).

Ventajosamente, un atacante no es consciente de los dominios de código y datos de personalización de seguridad que serán asignados a / almacenados en la aplicación software protegida de dispositivo móvil de un usuario dado, para habilitar los primeros dominios de código asignados para operación regular, lo cual hace extremadamente difícil tener éxito en un posterior ataque. Este ataque es incluso más complicado si se establecen límites de tiempo para realizar ciertos procesos sensibles de habilitación, como se ha descrito anteriormente.

Además, gracias al proceso de asignación impredecible de dominios de código y los diferentes datos de personalización de seguridad aplicados a la aplicación software protegida de dispositivo móvil en diferentes dispositivos móviles de usuarios, para habilitar para operación regular los primeros dominios de código asignados, el incentivo para un ataque masivo disminuye drásticamente.

También, la asignación de dominios de código y los datos de personalización de seguridad pueden ser modificados durante el ciclo de vida de una aplicación software protegida de dispositivo móvil instalada en el dispositivo móvil de un usuario dado, lo cual aumenta aún más la seguridad del sistema.

Las figuras 2k y 2l son relativas a algunas implementaciones donde una aplicación software protegida de dispositivo móvil es re personalizada en términos de seguridad durante su ciclo de vida. En particular, se refieren a un proceso de re personalización de seguridad de la aplicación software protegida de dispositivo móvil instalada en el dispositivo móvil del usuario 2 (como se ha explicado anteriormente dicha aplicación ya está personalizada en términos de seguridad en relación al registro de personalización de seguridad de ciclo de vida RPS32).

Conforme a algunas implementaciones una re personalización de seguridad es iniciada (ej. en el paso (17) de la figura 1) por uno o más dispositivos de procesamiento en el sistema del proveedor de servicios de personalización (ej. un periodo de tiempo después de que se haya realizado una personalización / re personalización de seguridad previa; ej. debido a criterios de riesgo).

Conforme a otras implementaciones el proceso de re personalización de seguridad es iniciado como resultado de una conexión on-line establecida (no ilustrado en la figura 1) desde el dispositivo móvil del usuario 2 hacia el sistema del proveedor de servicios de personalización. En un ejemplo particular una credencial dinámica basada-en-PIN es recibida desde el dispositivo móvil del usuario 2 durante la conexión on-line, y verificación con éxito de dicha credencia es requerida para que uno o más dispositivos de procesamiento del sistema del proveedor de servicios de personalización inicien (ej. en el paso (17) de la figura 1) el proceso de re personalización de seguridad.

Como se ilustra en la figura 1, en el paso (17) uno o más dispositivos de procesamiento en el sistema del proveedor de servicios de personalización obtienen datos de re personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida (ej. en el caso de que RPS32 contenga datos asociados a uno o más procesos de re personalización de seguridad), o a otro registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario, desde la base de datos asociada a aplicaciones software protegidas de dispositivo móvil.

En las implementaciones descritas a continuación, la re personalización de seguridad de la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 será realizada en relación al registro de personalización de seguridad de ciclo de vida RPS2j, por lo que en el paso (17) de la figura 1 el nuevo registro de personalización de seguridad de ciclo de vida asignado por el módulo de personalización de seguridad al dispositivo móvil del usuario 2 es RPS2j, que está asociado a DC2/1, DC2/2 y DC1. Todavía en el paso (17), la asignación del nuevo registro de personalización de seguridad de ciclo de vida RPS2j al dispositivo móvil del usuario 2 es almacenada en la base de datos asociada a aplicaciones software de dispositivo móvil (datos relativos a RPS32, asignados actualmente a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2, son todavía válidos, dado que en esta fase el proceso de re personalización todavía no ha sido realizado).

En más detalle (tomando también como referencia las figuras 2k y 2l), conforme a algunas implementaciones el módulo de personalización de seguridad puede realizar las siguientes nuevas asignaciones y preparación de datos en el paso (17) de la figura 1, en relación al dispositivo móvil del usuario 2 y a la re personalización de seguridad:

- Asignación de RPS2j en el contexto del proceso de re personalización de seguridad en curso, asociado a DC2/1, DC2/2 y DC1 y a $IDD_{USUARIO2}$;

- Asignar a $ps_{DCs\text{-}asignación}$ un valor de dato asociado a DC2/1 y DC2/2 tal que, una vez personalizado en términos de seguridad, la aplicación software protegida de dispositivo móvil usará DC2/1, DC2/2 y DC1 durante su ejecución. En estas implementaciones el valor de dato es ofuscado usando un método que usa un parámetro de seguridad que está embebido en una función DC1 y al menos parte de $IDD_{USUARIO2}$.

- Ofuscación de [$ps_{1b\text{-}RPS2j}$, $ro_{1b\text{-}RPS2j}$, $ch_{1b\text{-}RPS2j}$] usando un algoritmo de ofuscación y la clave de ofuscación para proteger datos de personalización de seguridad DC2/1, como se ilustra en la figura 2.k (en este proceso de personalización de seguridad x = 2). En estas implementaciones:

  - los primeros 10 dígitos de $IDD_{USUARIO2}$ son parte de la clave de ofuscación;

- [$ps_{1a\text{-}RS2}$, $ps_{1b\text{-}RPS2j}$] se convierten en las dos partes del mismo parámetro de seguridad:

  - Una o más partes de [$ps_{1a\text{-}RS2}$, $ps_{1b\text{-}RPS2j}$] serán usadas para validar que una solicitud para pre registrar un primer servicio (si dicho pre registro está pendiente), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC2/1 con la personalización de seguridad adecuada;

  - Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] serán usadas para proteger datos en ciertas partes de la base de datos de la aplicación software protegida de dispositivo móvil (en este contexto, ciertas partes asociadas a DC2/1 y DC2/2). En estas implementaciones, dichas otras una o más partes del parámetro de seguridad son usadas para proteger al menos parte de la parte de la base de datos de la aplicación que no está asociada a personalización / asignación de seguridad de dominios de código.

    Cuando la aplicación software protegida de dispositivo móvil recibe datos para almacenamiento en la al menos parte de la parte de la base de datos que no está asociada a personalización / asignación de seguridad de dominios de código, esos son cifrados usando las referidas otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$], antes de ser almacenados en la correspondiente al menos parte de la parte de la base de datos de la aplicación.

  - Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] son asignadas como el parámetro de seguridad que es parte de la clave de ofuscación usada para ofuscar [$ps_{2b\text{-}RPS2j}$], [$ch_{2b\text{-}RPS2j}$] y [$ro_{2b\text{-}RPS2j}$].

- [$ch_{1a\text{-}RS2}$, $ch_{1b\text{-}RPS2j}$] se convierten en las dos partes de la misma red de checksums, que será usada para verificar la integridad de partes del código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …).

  - En estas implementaciones $ch_{1b\text{-}RPS2j} = ch_{1b\text{-}RPS21}$;

  - Conforme a algunas implementaciones alternativas $ch_{1b\text{-}RPS2j} = ch_{1b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la red de checksums [$ch_{1a\text{-}RS2}$ / $ch_{1b\text{-}RPS2j}$] serán usadas para verificar la integridad de partes del código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …);

- [$ro_{1a\text{-}RS2}$, $ro_{1b\text{-}RPS2j}$] se convierten en las dos partes de la misma regla de ofuscación, que es usada para ofuscar parte del código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) junto con parte de los [$ps_{1a\text{-}RS2}$, $ps_{3\text{-}RS2,}$ $ps_{4\text{-}RS2}$ …, $ps_{g\text{-}RS2}$] y parte de los [$ch_{1a\text{-}RS2}$, $ch_{3\text{-}RS2,}$ $ch_{4\text{-}RS2}$ …, $ch_{g\text{-}RS2}$] embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …).

  - En estas implementaciones $ro_{1b\text{-}RPS2j} = ro_{1b\text{-}RPS21}$;

  - Conforme a algunas implementaciones alternativas $ro_{1b\text{-}RPS2j} = ro_{1b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{1a\text{-}RS2}$ / $ro_{1b\text{-}RPS2j}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la réplica de la función $fi_{DC2/1}$ en DC2/1 que está asociada al valor dado del parámetro.

- Ofuscación de [$ps_{2b\text{-}RPS2j}$, $ro_{2b\text{-}RPS2j}$, $ch_{2b\text{-}RPS2j}$] usando un algoritmo de ofuscación y la clave de ofuscación para proteger datos de personalización de seguridad DC2/2, como se ilustra en la figura 2.k (en este proceso de personalización de seguridad x = 2). En estas implementaciones:

  - El parámetro de seguridad que es parte de la clave de ofuscación está constituido por al menos parte de [$ps_{1a\text{-}RS2}$] y al menos parte de [$ps_{1b\text{-}RPS2j}$]. Los primeros 10 dígitos de $IDD_{USUARIO2}$ son también parte de la clave de ofuscación;

- [$ps_{2a\text{-}RS2}$, $ps_{2b\text{-}RPS2j}$] se convierten en las dos partes del mismo parámetro de seguridad:
  - Una o más partes de [$ps_{2a\text{-}RS2}$, $ps_{2b\text{-}RPS2j}$] serán usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC2/2 tras un pre registro previo con éxito del primer servicio, si dicho pre registro estaba pendiente), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC2/2 con la personalización de seguridad adecuada;
  - Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] serán usadas para proteger ciertos datos sensibles no estructurados antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 (ej. para proteger claves/datos sensibles necesarios para que la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 calcule credenciales dinámicas asociadas a servicios provistos por el proveedor de servicios 1; ej. protección de claves de sesión), cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DC2/1 y DC2/2.
  - Otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] serán usadas por la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 para ofuscar ciertos datos sensibles, en el contexto de la ejecución de algunas instrucciones de código DC2/2, para evitar que sean expuestas en claro en una o más memorias de trabajo del dispositivo móvil, cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DC2/1 y DC2/2.
- [$ch_{2a\text{-}RS2}$, $ch_{2b\text{-}RPS2j}$] se convierten en las dos partes de la misma red de checksums, que será usada para verificar la integridad de partes del código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …).
  - En estas implementaciones $ch_{2b\text{-}RPS2j} = ch_{2b\text{-}RPS21}$;
  - Conforme a algunas implementaciones alternativas $ch_{2b\text{-}RPS2j} = ch_{2b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la red de checksums [$ch_{2a\text{-}RS2}$ / $ch_{2b\text{-}RPS2j}$] serán usadas para verificar la integridad de partes del código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …);
- [$ro_{2a\text{-}RS2}$, $ro_{2b\text{-}RPS2j}$] se convierten en las dos partes de la misma regla de ofuscación, que son usadas para ofuscar parte del código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) junto con parte de los [$ps_{2a\text{-}RS2}$, $ps_{(g+1)\text{-}RS2,}$ $ps_{(g+2)\text{-}RS2}$ …, $ps_{m\text{-}RS2}$] y parte de los [$ch_{2a\text{-}RS2}$, $ch_{(g+1)\text{-}RS2,}$ $ch_{(g+2)\text{-}RS2}$ …, $ch_{m\text{-}RS2}$] embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …).
  - En estas implementaciones $ro_{2b\text{-}RPS2j} = ro_{2b\text{-}RPS21}$;
  - Conforme a algunas implementaciones alternativas $ro_{2b\text{-}RPS2j} = ro_{2b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{2a\text{-}RS2}$ / $ro_{2b\text{-}RPS2j}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas de la réplica de la función $fi_{DC2/2}$ en DC2/2 que está asociada al valor dado del parámetro.

Estas asignaciones y datos preparados son almacenados en la base de datos asociada a aplicaciones software protegidas de dispositivo móvil, en relación al dispositivo móvil del usuario 2, la aplicación software protegida de dispositivo móvil y el proceso de re personalización de seguridad.

En el paso (18) de la figura 1 datos de re personalización de seguridad asociados al nuevo registro de personalización de seguridad de ciclo de vida asignado (RPS2j) son enviados desde el proveedor de servicios de personalización a la aplicación software protegida de dispositivo móvil (en el dispositivo móvil del usuario 2) estando en un estado de seguridad parcialmente personalizada o personalizada, los datos de re personalización de seguridad son al menos parcialmente diferentes que los datos de personalización de seguridad. Conforme a algunas implementaciones (en relación a las figuras 2.k y 2.l) [$ps_{1b\text{-}RPS2j}$, $ro_{1b\text{-}RPS2j}$, $ch_{1b\text{-}RPS2j}$] y [$ps_{2b\text{-}RPS2j}$, $ro_{2b\text{-}$

$_{RPS2j}$, $ch_{2b\text{-}RPS2j}$] son enviados en formato ofuscado a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2.

En el paso (19) de la figura 1 el dispositivo móvil del usuario 2 recibe los datos de re personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida, o a otro registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario, en la aplicación software protegida de dispositivo móvil estando en un estado de seguridad parcialmente personalizada o personalizada, los datos de re personalización de seguridad son al menos parcialmente diferentes que los datos de personalización de seguridad y habilitan en la aplicación para operación regular al menos uno de los uno o más primeros dominios de código y/o al menos uno del otro uno o más primeros dominios de código. Ventajosamente, en esta invención al menos parte de la protección de seguridad puede ser renovada de vez en cuando o bajo ciertas circunstancias.

Conforme a algunas implementaciones (en relación a la figura 2.l) el dispositivo móvil del usuario 2 recibe en formato ofuscado (la ofuscación usando un método que usa un parámetro de seguridad que está embebido en una función de DC1 y al menos parte de $IDD_{USUARIO2}$) desde el proveedor de servicios de personalización el valor de dato para almacenamiento en la parte de la aplicación software protegida de dispositivo móvil asociada a $ps_{DCs\text{-}asignación}$, dicho valor haciendo que la aplicación software protegida de dispositivo móvil use DC2/1, DC2/2 y DC1 durante su ejecución (y que por tanto deje de usar DC3/1 y CD3/2 durante su ejecución).

En estas implementaciones el dispositivo móvil del usuario 2 también recibe [$ps_{1b\text{-}RPS2j}$, $ro_{1b\text{-}RPS2j}$, $ch_{1b\text{-}RPS2j}$] y [$ps_{2b\text{-}RPS2j}$, $ro_{2b\text{-}RPS2j}$, $ch_{2b\text{-}RPS2j}$] en formato ofuscado desde el proveedor de servicios de personalización y estos son respectivamente almacenados en la parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a DC2/1 y DC 2/2 (como se ilustra en la figura 2.l).

Los datos de personalización de seguridad [$ps_{1b\text{-}RPS2j}$, $ro_{1b\text{-}RPS2j}$, $ch_{1b\text{-}RPS2j}$] recibidos y almacenados habilitan el primer dominio de código DC2/1 para operación regular, la ofuscación de los datos [$ps_{1b\text{-}RPS2j}$, $ro_{1b\text{-}RPS2j}$, $ch_{1b\text{-}RPS2j}$] siendo relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en el segundo dominio de código DC1 y que son requeridos para habilitar el primer dominio de código DC2/1 para operación regular, como se ha ilustrado parcialmente antes en relación a la figura 2.k (x = 2).

Los datos de personalización de seguridad [$ps_{2b\text{-}RPS2j}$, $ro_{2b\text{-}RPS2j}$, $ch_{2b\text{-}RPS2j}$] recibidos y almacenados habilitan el otro primer dominio de código DC2/2 para operación regular, la ofuscación de los datos [$ps_{2b\text{-}RPS2j}$, $ro_{2b\text{-}RPS2j}$, $ch_{2b\text{-}RPS2j}$] siendo relativa al parámetro de seguridad (otras una o más partes de [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$]) que es parte de la clave de ofuscación que protege datos de re personalización de seguridad DC2/2, como se ha ilustrado anteriormente en relación a la figura 2.k (x = 2).

En el contexto descrito en las figuras 2.k y 2.l, DC2/2 es el al menos uno del otro uno o más primeros dominios de código. En relación a la re personalización de seguridad asociada al registro de personalización de seguridad de ciclo de vida RPS2j y al dispositivo móvil del usuario 2, el al menos uno del otro uno o más primeros dominios de código (DC2/2) está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código (DC2/1) a través de la re personalización de seguridad ([$ps_{2b\text{-}RPS2j}$, $ro_{2b\text{-}RPS2j}$, $ch_{2b\text{-}RPS2j}$] en formato ofuscado), dicha re personalización relativa a parámetros de seguridad (al menos parte de [$ps_{1a\text{-}RS2}$, $ps_{1b\text{-}RPS2j}$]) y/o reglas de ofuscación (al menos parte de [$ro_{1a\text{-}RS2}$, $ro_{1b\text{-}RPS2j}$]) y/o datos de checksums de código (al menos parte de [$ch_{1a\text{-}RS2}$, $ch_{1b\text{-}RPS2j}$]) que están al menos parcialmente disponibles en los uno o más primeros dominios de código (DC2/1) y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

También en el contexto de la re personalización de seguridad asociada al registro de personalización de seguridad de ciclo de vida RPS2j y al dispositivo móvil del usuario 2, al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados a una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a los uno o más primeros dominios de código ([$ps_{1b\text{-}RPS2j}$]) y/o [$ro_{1b\text{-}RPS2j}$]) y/o [$ch_{1b\text{-}RPS2j}$] están disponibles en una parte de la base de datos de la aplicación que está asociada a DC2/1).

También, en el proceso de re personalización de seguridad, en relación al dispositivo móvil del usuario 2, conforme a algunas implementaciones:

- La parte de la base de datos de la aplicación software protegida de dispositivo móvil asociada a datos de personalización de seguridad DC3/1 y DC3/2 es establecida a valores por defecto [$ps_{1b\text{-}RPS3VD}$, $ro_{1b\text{-}RPS3VD}$, $ch_{1b\text{-}RPS3VD}$] y [$ps_{2b\text{-}RPS3VD}$, $ro_{2b\text{-}RPS3VD}$, $ch_{2b\text{-}RPS3VD}$], como se ilustra en la figura 2.I.

- Datos en ciertas partes de la base de datos de la aplicación software protegida de dispositivo móvil, previamente protegidos por las otras unas o más partes del parámetro de seguridad [$ps_{1a\text{-}RS3}$ / $ps_{1b\text{-}RPS32}$] (relativos a la "antigua" personalización de seguridad asociada a DC3/1 y DC3/2) son borrados y dichos datos son al menos parcialmente reemplazados durante el proceso de re personalización (tanto como sea posible / necesario) con datos de renovación enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario 2. Como ya se ha dicho anteriormente cuando esos datos de renovación son recibidos, otras una o más partes de [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] serán usadas para proteger los datos de renovación en dichas ciertas partes de la base de datos de la aplicación software protegida de dispositivo móvil (en este contexto de re personalización, ciertas partes asociadas a DC2/1 y DC2/2).

  En estas implementaciones, dichas otras una o más partes de [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] son usadas para proteger al menos parte de la parte de la base de datos de la aplicación que no está asociada a personalización / asignación de seguridad de dominios de código. En relación a la re personalización de seguridad, cuando la aplicación software protegida de dispositivo móvil recibe datos (del proveedor de servicios de personalización o de otras fuentes) para almacenamiento en la al menos parte de la parte de la base de datos que no está asociada a personalización / asignación de seguridad de dominios de código, esos son cifrados usando las referidas otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$], antes de ser almacenados en la correspondiente al menos parte de la parte de la base de datos de la aplicación.

- Ciertos datos sensibles no estructurados almacenados en la base de datos de la aplicación software protegida de dispositivo móvil, protegidos previamente por las otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS3}$ / $p_{2b\text{-}RPS32}$] (relativos a la "antigua" personalización de seguridad asociada a DC3/1 y DC3/2) son borrados y dichos datos son reemplazados durante el proceso de re personalización (tanto como sea posible / necesario) por ciertos datos sensibles no estructurados de renovación enviados desde el proveedor de servicios de personalización al dispositivo móvil del usuario 2.

  En relación a la re personalización de seguridad, otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] serán usados para proteger dichos datos sensibles no estructurados de renovación antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 (ej. para proteger claves/ datos sensibles necesarios para que la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2 calcule credenciales dinámicas asociadas a servicios provistos por el proveedor de servicios 1; ej. protección de claves de sesión) , cuando $ps_{DCs\text{-}asignación}$ es establecido al valor asociado a DC2/1 y DC2/2.

Ventajosamente, después de que la re personalización de seguridad anterior haya sido realizada, el referido al menos uno de los uno o más primeros dominios de código (DC2/1) y el al menos uno del otro uno o más primeros dominios de código (DC2/2) pueden ser usados para realizar regularmente las funciones asociadas de ciclo de vida de la aplicación.

Una vez que el proceso de re personalización de seguridad ha finalizado con éxito, en un paso posterior (no ilustrado en la figura 1) los datos enviados al proveedor de servicios 1 en el contexto del paso (11) de la figura 1 son actualizados. Conforme a algunas implementaciones al menos parte de las asignaciones y/o datos asociados al dispositivo móvil del usuario 2 y a la re personalización de seguridad de la aplicación software protegida de dispositivo móvil son enviados al proveedor de servicios 1 para almacenamiento y para uso de al menos parte de ellos en el contexto de ciertos procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil asociada al dispositivo móvil del usuario 2. En un ejemplo particular:

- La una o más partes de [$ps_{1a\text{-}RS2}$, $ps_{1b\text{-}RPS2j}$] que serán usadas para validar que una solicitud para pre registrar un primer servicio (si dicho pre registro están pendiente), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC2/1 con la personalización de seguridad adecuada y;

- Las una o más partes de [$ps_{2a\text{-}RS2}$, $ps_{2b\text{-}RPS2j}$] que serán usadas para validar que una solicitud para registrar el primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC2/2 tras un pre registro previo con éxito del primer servicio, si dicho pre registro estaba pendiente), asociado al proveedor de servicios 1, en la aplicación software protegida de dispositivo móvil es recibida desde

el dispositivo móvil del usuario 2 (con $IDD_{USUARIO2}$) y ha sido lanzada desde DC2/2 con la personalización de seguridad adecuada;

son enviadas al proveedor de servicios 1 para almacenamiento y para uso durante el proceso de pre registro y de registro, respectivamente, de un primer servicio (si pendiente) en la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2.

Durante su ciclo de vida la aplicación software protegida de dispositivo móvil re personalizada en seguridad será capaz de des ofuscar $ps_{DCs\text{-}asignación}$ y de determinar que DC2/1, DC2/2 y DC1 deben ser usados durante su ejecución. También, la aplicación software protegida de dispositivo móvil será capaz de des ofuscar [$ps_{1b\text{-}RPS2j}$, $ro_{1b\text{-}RPS2j}$, $ch_{1b\text{-}RPS2j}$] usando el algoritmo de ofuscación y la clave de ofuscación que protege datos de personalización de seguridad DC2/1, como ya se ha ilustrado en relación a la figura 2.k (x = 2). Más en detalle:

- Para solicitar el pre registro de un primer servicio (si pendiente), una o más partes de [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil, y un cálculo basado en las una o más partes des ofuscadas de [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] es enviado al proveedor de servicios 1 para verificación de que la solicitud es enviada desde el dispositivo apropiado y ha sido lanzada desde el dominio de código adecuado (DC2/1) con la correcta personalización de seguridad. Como se ha referido anteriormente, el proveedor de servicios 1 ha almacenado previamente las una o más partes de [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] en relación al dispositivo móvil del usuario 2, para usarlas durante el proceso de verificación.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] son usadas para proteger al menos parte de la parte de la base de datos de la aplicación asociada a DC2/1 y DC2/2 (y no asociada a personalización / asignación de seguridad de dominios de código). Cuando la aplicación software protegida de dispositivo móvil requiere del uso de datos almacenados en dicha al menos parte de la parte de la base de datos, las otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar los datos en la base de datos, para uso.

- Otras una o más partes del parámetro de seguridad [$ps_{1a\text{-}RS2}$ / $ps_{1b\text{-}RPS2j}$] serán des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para calcular la clave de ofuscación para des ofuscar [$ps_{2b\text{-}RPS2j}$], [$ch_{2b\text{-}RPS2j}$] y [$ro_{2b\text{-}RPS2j}$], cuando sea requerido.

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ch_{1a\text{-}RS2}$, $ch_{1b\text{-}RPS2j}$] serán usados para verificar la integridad de las partes relativas del código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{1a\text{-}RS2}$, $ch_{1b\text{-}RPS2j}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. Como se ha referido anteriormente, en estas implementaciones $ch_{1b\text{-}RPS2j}$ = $ch_{1b\text{-}RPS21}$;

  - Conforme a las implementaciones alternativas referidas anteriormente, $ch_{1b\text{-}RPS2j}$ = $ch_{1b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ ha sido establecido a un valor dado tal que una o más partes asociadas de la red de checksums [$ch_{1a\text{-}RS2}$ / $ch_{1b\text{-}RPS2j}$] serán usadas para verificar la integridad de partes relativas del código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …) y de al menos partes relativas de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …);

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ro_{1a\text{-}RS2}$, $ro_{1b\text{-}RPS2j}$] será usada para des ofuscar la parte relativa del código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …), la parte relativa de los [$ps_{1a\text{-}RS2}$, $ps_{3\text{-}RS2,}$ $ps_{4\text{-}RS2}$ …, $ps_{g\text{-}RS2}$] y la parte relativa de los [$ch_{1a\text{-}RS2}$, $ch_{3\text{-}RS2,}$ $ch_{4\text{-}RS2}$ …, $ch_{g\text{-}RS2}$] embebidos en el código de la aplicación de las funciones DC2/1($f1_{DC2/1}$, $f2_{DC2/1,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha parte referida del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{1a\text{-}RS2}$ / $ro_{1b\text{-}RPS2j}$]. Como se ha referido anteriormente, en estas implementaciones ro1b-RPS2j = ro1b-RPS21;

  - Conforme a las implementaciones alternativas referidas anteriormente $ro_{1b\text{-}RPS2j}$ = $ro_{1b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{1a\text{-}RS2}$ / $ro_{1b\text{-}RPS2j}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos de la réplica de la

función $fi_{DC2/1}$ en DC2/1 que está asociada al valor dado del parámetro cuando la aplicación software protegida de dispositivo móvil requiere el uso de dicha parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos.

También, durante su ciclo de vida la aplicación software protegida de dispositivo móvil re personalizada en seguridad será capaz de des ofuscar [$ps_{2b\text{-}RPS2j}$, $ro_{2b\text{-}RPS2j}$, $ch_{2b\text{-}RPS2j}$] usando el algoritmo de ofuscación y la clave de ofuscación que protege datos de personalización de seguridad DC2/2, como ya se ha ilustrado en relación a la figura 2k (x = 2). Más en detalle:

- Para solicitar el registro del primer servicio referido anteriormente (la solicitud de registro siendo lanzada desde DC2/2 tras un pre registro previo con éxito del primer servicio, si dicho pre registro estaba pendiente), una o más partes de [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil, y un cálculo basado en las des ofuscadas una o más partes de [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] es enviado al proveedor de servicios 1 para verificación de que la solicitud es enviada desde el dispositivo apropiado y ha sido lanzada desde el dominio de código adecuado (DC2/2) con la personalización de seguridad adecuada. Como se ha referido anteriormente, el proveedor de servicios 1 ha almacenado previamente las una o más partes de [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] en relación al dispositivo móvil del usuario 2, para usarlas durante el proceso de verificación.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] son usadas para proteger ciertos datos sensibles no estructurados antes de ser enviados para almacenamiento a la aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario 2. Conforme a algunas implementaciones cuando la aplicación software protegida de dispositivo móvil requiere el uso de al menos parte de los datos sensibles no estructurados, las otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] son des ofuscadas por la aplicación software protegida de dispositivo móvil para usarlas para descifrar los al menos parte de los datos sensibles no estructurados almacenados, para uso.

- Como se ha detallado anteriormente, otras una o más partes del parámetro de seguridad [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] son usadas para ofuscar ciertos datos sensibles, en el contexto de la ejecución de algunas instrucciones de código DC2/2, para evitar que sean expuestos en claro en una o más memorias de trabajo del dispositivo móvil del usuario 2. Cuando, durante la ejecución de ciertas instrucciones de código DC2/2, uno o más dispositivos de procesamiento en el dispositivo móvil del usuario 2 requieren usar los datos sensibles ofuscados previamente almacenados en las una o más memorias de trabajo, estos utilizan las otras una o más partes de [$ps_{2a\text{-}RS2}$ / $ps_{2b\text{-}RPS2j}$] (y la regla de ofuscación referida anteriormente en relación a la figura 2.b) para obtener los datos adecuados para el relativo cálculo/proceso.

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ch_{2a\text{-}RS2}$, $ch_{2b\text{-}RPS2j}$] será usado para verificar la integridad de las partes relativas del código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) y de al menos partes de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere verificar la referida integridad, la red de checksums [$ch_{2a\text{-}RS2}$, $ch_{2b\text{-}RPS2j}$] es des ofuscada por la aplicación software protegida de dispositivo móvil para usarla en el proceso de verificación. Como se ha referido anteriormente, en estas implementaciones $ch_{2b\text{-}RPS2j} = ch_{2b\text{-}RPS21}$;

  - Conforme a las implementaciones alternativas referidas anteriormente, $ch_{2b\text{-}RPS2j} = ch_{2b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ ha sido establecido a un valor dado tal que una o más partes asociadas de la red de checksums [$ch_{2a\text{-}RS2}$ / $ch_{2b\text{-}RPS2j}$] serán usadas para verificar la integridad de partes relativas del código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …) y de al menos partes relativas de uno o más parámetros de seguridad embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …);

- Durante el ciclo de vida de la aplicación software protegida de dispositivo móvil, [$ro_{2a\text{-}RS2}$, $ro_{2b\text{-}RPS2j}$] será usada para des ofuscar la parte relativa del código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …), la parte relativa de los [$ps_{2a\text{-}RS2}$, $ps_{(g+1)\text{-}RS2,}$ $ps_{(g+2)\text{-}RS2}$ …, $ps_{m\text{-}RS2}$] y la parte relativa de los [$ch_{2a\text{-}RS2}$, $ch_{(g+1)\text{-}RS2,}$ $ch_{(g+2)\text{-}RS2}$ …, $ch_{m\text{-}RS2}$] embebidos en el código de la aplicación de las funciones DC2/2($f1_{DC2/2}$, $f2_{DC2/2,}$ …). Cuando la aplicación software protegida de dispositivo móvil requiere usar dicha referida parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas, el correspondiente proceso de des ofuscación es aplicado usando [$ro_{2a\text{-}RS2}$ / $ro_{2b\text{-}RPS2j}$]. Como se ha referido anteriormente, en estas implementaciones $ro_{2b\text{-}RPS2j} = ro_{2b\text{-}RPS21}$;

- Conforme a las implementaciones alternativas referidas anteriormente $ro_{2b\text{-}RPS2j} = ro_{2b\text{-}RPS21}$ y un parámetro en $ps_{DCs\text{-}asignación}$ es establecido a un valor dado tal que una o más partes de la regla de ofuscación [$ro_{2a\text{-}RS2}$ / $ro_{2b\text{-}RPS2j}$] (esas partes asociadas al valor dado del parámetro) serán usadas para des ofuscar por la aplicación software protegida de dispositivo móvil una parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidos de la réplica de la función $fi_{DC2/2}$ en DC2/2 que está asociada al valor dado del parámetro cuando la aplicación software protegida de dispositivo móvil requiere el uso de dicha parte del código de la aplicación / parámetros de seguridad embebidos / redes de checksums embebidas.

Esta invención provee un gran número de métodos y técnicas asociadas a uno o más proveedores de servicios y un proveedor de servicios de personalización en relación a la personalización de seguridad de una aplicación software de dispositivo móvil en un dispositivo móvil de un usuario.

Aunque se han descrito en detalle implementaciones de ejemplo para el propósito ilustrativo, se entiende que dicho detalle es solo para ese propósito, y que se pueden realizar variaciones en las mismas por aquellos expertos en la técnica sin apartarse del ámbito de la invención.

En una implementación particular la aplicación software protegida de dispositivo móvil es relativa a varios proveedores de servicios y una arquitectura equivalente a la ilustrada en la figura 2.b es replicada en el código de aplicación para cada uno de los proveedores de servicios.

Por tanto, ventajosamente cada proveedor de servicios puede tener sus propios primeros y segundos dominios de código asociados en la aplicación software protegida de dispositivo móvil, la parte asociada en la base de datos de la aplicación, registros de personalización de seguridad asociados, y personalización de seguridad aplicada en dispositivos móviles de los usuarios; conforme a algunas implementaciones (como se ilustra en la figura 3) el código de aplicación asociado a un proveedor de servicios dado en la aplicación software protegida de dispositivo móvil puede estar completamente aislado del código de aplicación asociado a otro proveedor de servicios dado.

La implementación ilustrada en la figura 3 se refiere a cuatro proveedores de servicios, cada uno con su propio registro de personalización de seguridad de inicialización (RPS-I_{PS1}, RPS-I_{PS2}, RPS-I_{PS3}, RPS-I_{PS4}). El registro de personalización de seguridad de inicialización de la aplicación incluye RPS-I_{PS1}, RPS-I_{PS2}, RPS-I_{PS3} y RPS-I_{PS4} y la protección de seguridad aplicada a la aplicación puede ser testada primero usando RPS-I_{PS1} (como se describe ej. en relación a la figura 2.b) para testar la parte de la aplicación asociada al proveedor de servicios 1; segundo usando RPS-I_{PS2}, para testar la parte de la aplicación asociada al proveedor de servicios 2; tercero usando RPS-I_{PS3}, para testar la parte de la aplicación asociada al proveedor de servicios 3; y finalmente usando RPS-I_{PS4}, para testar la parte de la aplicación asociada al proveedor de servicios 4;

Los pasos 8 a 19 descritos en la figura 1 pueden ser independientemente realizados en relación a los primeros y segundos dominios de código asociados a cada uno de los proveedores de servicios. La figura 3 muestra un ejemplo donde $RPS2j_{PS1}$ ha sido usado para personalizar en términos de seguridad la parte de la base de datos de la aplicación software protegida de dispositivo móvil asociada a $DC2/1_{PS1}$ y $DC2/2_{PS1}$; la figura 3 también muestra un ejemplo donde $RPSn3_{PS4}$ ha sido usado para personalizar en términos de seguridad la parte de la base de datos de la aplicación software protegida de dispositivo móvil asociada a $DCn/1_{PS4}$ y $DCn/2_{PS4}$.

Ventajosamente, conforme a algunas implementaciones uno o más primeros dominios de código asociados a un primer proveedor de servicios (ej. proveedor de servicios 1) pueden ser habilitados para operación regular por el proveedor de servicios de personalización independientemente de la habilitación para operación regular de otros uno o más primeros dominios de código asociados a un segundo proveedor de servicios (ej. proveedor de servicios 4).

Más allá, aunque las implementaciones reveladas en este documento con referencia a los dibujos comprenden aparatos y procesos informáticos realizados en aparatos informáticos, la invención también se extiende a programas informáticos, particularmente programas informáticos sobre o en un soporte, adaptados para poner la invención en práctica. El programa puede estar en forma de código fuente, código objeto, una fuente intermedia de código y código objeto tal como en forma parcialmente compilada, o en cualquier otra forma adecuada para su uso en la implementación de los procesos de acuerdo con la invención. El soporte puede ser cualquier entidad o dispositivo capaz de llevar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, como una ROM, por ejemplo, un CD ROM o una ROM semiconductora, o un medio de grabación magnético, por ejemplo, un disquete o un disco duro. Además, el soporte puede ser un portador transmisible tal como una señal eléctrica u óptica que puede ser transportada mediante cable eléctrico u óptico o por radio u otros medios. Cuando el programa se materializa en una señal que puede ser transmitida

directamente por un cable u otro dispositivo o medio, el soporte puede estar constituido por dicho cable u otro dispositivo o medio. Alternativamente, el soporte puede ser un circuito integrado en el que está incrustado el programa, estando adaptado el circuito integrado para realizar, o para uso en la ejecución de, los procesos relevantes.

REIVINDICACIONES

1. Un método asociado con uno o más proveedores de servicios y un proveedor de servicios de personalización en relación a la personalización de seguridad de una aplicación software de dispositivo móvil en un dispositivo móvil de un usuario, el método incluyendo:

usando por el proveedor de servicios de personalización una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad que están almacenados en una o más memorias para generar usando uno o más dispositivos de procesamiento una aplicación software protegida de dispositivo móvil que es personalizada en términos de seguridad usando datos del registro de personalización de seguridad, la aplicación generada incluyendo varios dominios de código, relativos a los uno o más proveedores de servicios, donde uno o más primeros dominios de código son vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar los uno o más primeros dominios de código para operación regular;

enviando la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada desde el proveedor de servicios de personalización a un servidor de distribución, dicho estado deshabilitando los uno o más primeros dominios de código para operación regular, y la aplicación software protegida de dispositivo móvil siendo almacenada en una o más memorias del servidor de distribución;

recibiendo desde el dispositivo móvil del usuario una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada;

enviando datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario, a la aplicación software protegida de dispositivo móvil no personalizada en seguridad en el dispositivo móvil del usuario, los datos de personalización de seguridad habilitando en la aplicación al menos uno de los uno o más primeros dominios de código para operación regular.

2. Un método conforme a la reivindicación 1, en donde el proveedor de servicios de personalización es uno de los uno o más proveedores de servicios.

3. Un método conforme a las reivindicaciones 1 o 2, en donde el habilitado de el al menos uno de los uno o más primeros dominios de código está asociado a uno o más parámetros de seguridad relativos al registro de personalización de seguridad de ciclo de vida, que son diferentes que los correspondientes del registro de personalización de seguridad.

4. Un método conforme a cualquiera de las reivindicaciones 1 a 3, en donde la personalización de seguridad asociada al registro de personalización de seguridad de ciclo de vida es relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

5. Un método conforme a cualquiera de las reivindicaciones 1 a 4, en donde solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código son recibidas desde el dispositivo móvil del usuario, cada solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida son enviados a la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

6. Un método conforme a la reivindicación 5, en donde al menos uno del otro uno o más primeros dominios de código está vinculado en términos de seguridad por el proveedor de servicios de personalización a uno o más primeros dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

7. Un método conforme a la reivindicación 6, en donde al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular han sido previamente enviados a una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a los uno o más primeros dominios de código.

8. Un método conforme a cualquiera de las reivindicaciones 5 a 7, en donde uno o más dispositivos de procesamiento hacen una aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad expirar si una solicitud para una personalización de seguridad de al menos otro uno o más primeros dominios de código es recibida más tarde que un periodo de tiempo predefinido después de que datos de personalización de seguridad relativos a una solicitud previa para una personalización de seguridad de al menos uno u otro diferente uno de los uno o más primeros dominios de código fueran enviados a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada o parcialmente-personalizada.

9. Un método conforme a cualquiera de las reivindicaciones 1 a 8, en donde datos de re personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida, o a otro registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario, son enviados a la aplicación software protegida de dispositivo móvil estando en un estado de seguridad parcialmente-personalizada o personalizada, los datos de re personalización de seguridad son al menos parcialmente diferentes que los datos de personalización de seguridad y habilitan en la aplicación para operación regular al menos uno de los uno o más primeros dominios de código y/o al menos uno del otro uno o más primeros dominios de código.

10. Un método conforme a cualquiera de las reivindicaciones 1 a 9, en donde uno o más primeros dominios de código asociados a un primer proveedor de servicios pueden ser habilitados para operación regular por el proveedor de servicios de personalización independientemente de la habilitación para operación regular de otros uno o más primeros dominios de código asociados a un segundo proveedor de servicios.

11. Un método asociado con el uso de un dispositivo móvil de un usuario en relación a la personalización de seguridad de una aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario, la aplicación software protegida de dispositivo móvil previamente generada por un proveedor de servicios de personalización en un estado de seguridad personalizada usando una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad, la aplicación protegida incluyendo varios dominios de código, relativos a uno o más proveedores de servicios, donde uno o más primeros dominios de código quedan vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad asociada al registro de personalización de seguridad, el método incluyendo:

solicitando desde el dispositivo móvil del usuario una aplicación software de dispositivo móvil a un servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada;

recibiendo desde el servidor de distribución y a continuación instalando por uno o más dispositivos de procesamiento en el dispositivo móvil la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código están deshabilitados para operación regular;

enviando desde el dispositivo móvil del usuario una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estado en un estado de seguridad no-personalizada;

recibiendo datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no-personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos

dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

12. Un método conforme a la reivindicación 11, en donde solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código son enviadas desde el dispositivo móvil del usuario al proveedor de servicios de personalización, cada solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario son recibidos en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

13. Un método conforme a la reivindicación 12, en donde al menos uno del otro uno o más primeros dominios de código está vinculado en términos de seguridad a uno o más primeros dominios de código a través de la personalización de seguridad, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más primeros dominios de código y que son requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular.

14. Un método conforme a la reivindicación 13, en donde al menos parte de los parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código requeridos para habilitar el al menos uno del otro uno o más primeros dominios de código para operación regular están disponibles en una parte de la base de datos de la aplicación software protegida de dispositivo móvil que está asociada a uno o más primeros dominios de código que han sido previamente habilitados para operación regular.

15. Un método conforme a cualquiera de las reivindicaciones 11 a 14, en donde el uno o más primeros dominios de código habilitados mediante primeros datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un primer usuario son diferentes que los uno o más primeros dominios de código habilitados mediante segundos datos de personalización de seguridad recibidos en la aplicación software protegida de dispositivo móvil instalada en un dispositivo móvil de un segundo usuario.

16. Un método conforme a cualquiera de las reivindicaciones 11 a 15, en donde los datos de personalización de seguridad recibidos en el dispositivo móvil de un primer usuario, los datos habilitando en la aplicación uno o más primeros dominios de código para operación regular y asociados a un primer registro de personalización de seguridad de ciclo de vida que incluye primeros parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código, son diferentes que los datos de personalización de seguridad recibidos en el dispositivo móvil de un segundo usuario, los datos habilitando en la aplicación uno o más primeros dominios de código para operación regular y asociados a un segundo registro de personalización de seguridad de ciclo de vida que incluye segundos parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código.

17. Un medio leíble no transitorio de ordenador almacenando código leíble de programa de ordenador para causar un procesador de un dispositivo móvil de un usuario realizar un método asociado a la personalización de seguridad de una aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario, la aplicación software protegida de dispositivo móvil previamente generada por un proveedor de servicios de personalización en un estado de seguridad personalizada usando una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad, la aplicación protegida incluyendo varios dominios de código, relativos a uno o más proveedores de servicios, donde uno o más primeros dominios de código quedan vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad asociada al registro de personalización de seguridad, el método incluyendo:

solicitando desde el dispositivo móvil del usuario una aplicación software de dispositivo móvil a un servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no-personalizada;

recibiendo desde el servidor de distribución y a continuación instalando por uno o más dispositivos de procesamiento en el dispositivo móvil la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código están deshabilitados para operación regular;

enviando desde el dispositivo móvil del usuario una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estado en un estado de seguridad no-personalizada;

recibiendo datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no-personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

18. Un medio leíble no transitorio de ordenador almacenando código leíble de programa de ordenador conforme a la reivindicación 17 que causa el procesador enviando solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código desde el dispositivo móvil del usuario al proveedor de servicios de personalización, cada solicitud siendo lanzada por uno o más dispositivos de procesamiento utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y recibiendo datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

19. Un dispositivo móvil de un usuario asociado con la personalización de seguridad de una aplicación software protegida de dispositivo móvil en el dispositivo móvil del usuario, la aplicación software protegida de dispositivo móvil previamente generada por un proveedor de servicios de personalización en un estado de seguridad personalizada usando una aplicación software de dispositivo móvil, un registro de personalización de seguridad y software de protección de seguridad, la aplicación protegida incluyendo varios dominios de código, relativos a uno o más proveedores de servicios, donde uno o más primeros dominios de código quedan vinculados en términos de seguridad a uno o más segundos dominios de código a través de la personalización de seguridad asociada al registro de personalización de seguridad, el dispositivo móvil incluyendo:

un medio de almacenamiento electrónico que almacena datos de personalización de seguridad; y
un procesador adaptado a:

solicitar una aplicación software de dispositivo móvil a un servidor de distribución, el servidor de distribución almacenando en una o más memorias la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no personalizada;

recibir desde el servidor de distribución y a continuación instalar en el dispositivo móvil la aplicación software protegida de dispositivo móvil en un estado de seguridad no-personalizada, en donde en dicho estado de personalización de seguridad pendiente los uno o más primeros dominios de código estas deshabilitados para operación regular;

enviar una solicitud para una personalización de seguridad de al menos uno de los uno o más primeros dominios de código, la solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más segundos dominios de código de la aplicación software protegida de dispositivo móvil estando en un estado de seguridad no personalizada;

recibir datos de personalización de seguridad asociados a un registro de personalización de seguridad de ciclo de vida que es relativo al dispositivo móvil del usuario desde el proveedor de servicios de personalización, los datos de personalización de seguridad habilitando en la aplicación software protegida de dispositivo móvil no-personalizada en seguridad al menos uno de los uno o más primeros dominios de código para operación regular, dicha personalización relativa a parámetros de seguridad y/o reglas de ofuscación y/o datos de checksums de código que están al menos parcialmente disponibles en los uno o más segundos dominios de código y que son requeridos para habilitar el al menos uno de los uno o más primeros dominios de código para operación regular.

20. Un dispositivo móvil de un usuario conforme a la reivindicación 19, en donde el procesador está adaptado para enviar solicitudes sucesivas para una personalización de seguridad de al menos otro uno o más primeros dominios de código desde el dispositivo móvil del usuario al proveedor de servicios de personalización, cada solicitud siendo lanzada utilizando código ejecutable perteneciente a uno de los uno o más primeros dominios de código que han sido previamente habilitados para operación regular, y para recibir datos de personalización de seguridad asociados al registro de personalización de seguridad de ciclo de vida relativo al dispositivo móvil del usuario en la aplicación software protegida de dispositivo móvil parcialmente personalizada en seguridad, los datos de personalización de seguridad habilitando en la aplicación para operación regular el al menos otro uno o más primeros dominios de código que está asociado a la solicitud particular.

Figura 1

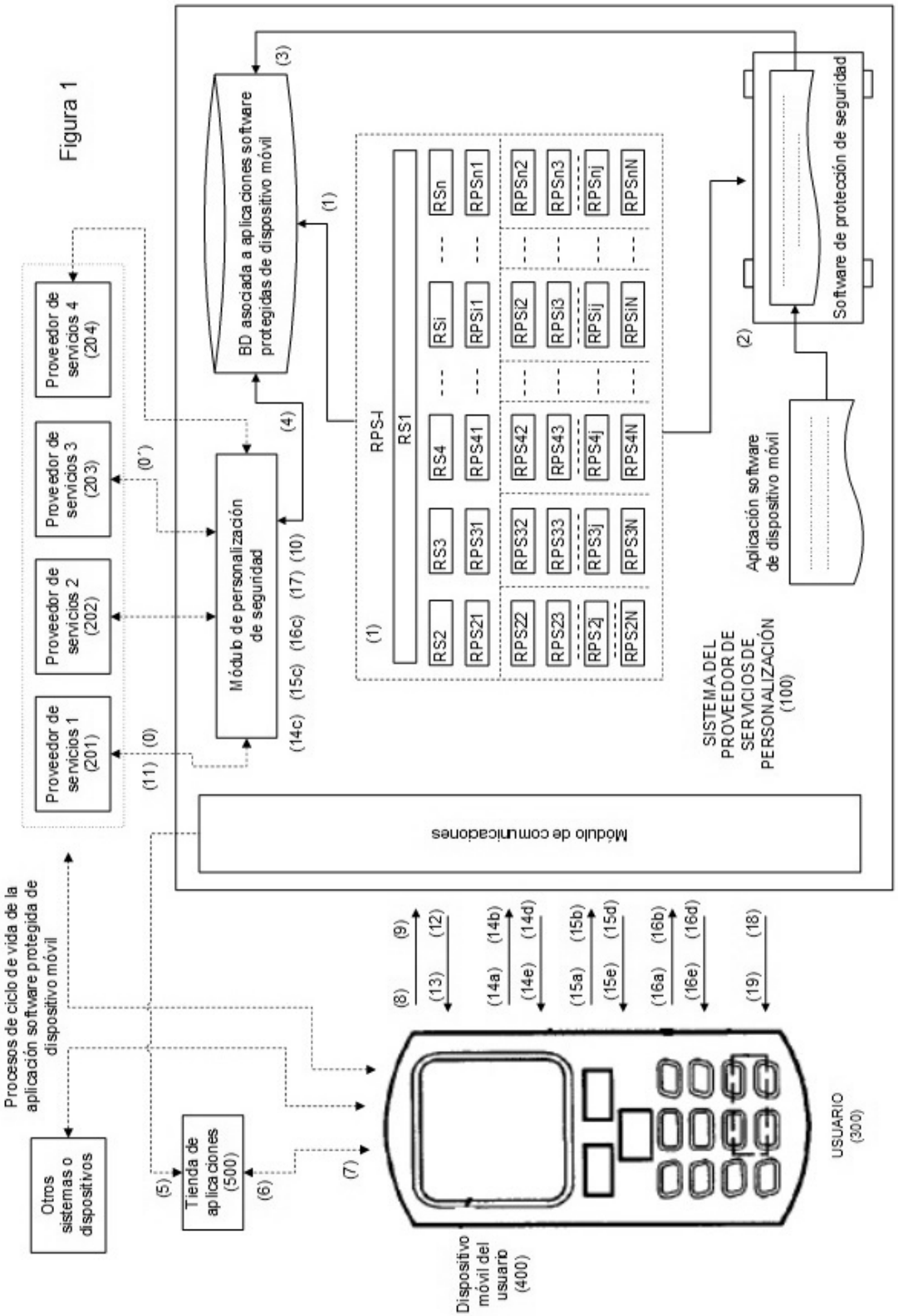

Procesos de ciclo de vida de la aplicación software protegida de dispositivo móvil
Otros sistemas o dispositivos
Tienda de aplicaciones (500)
Dispositivo móvil del usuario (400)
USUARIO (300)
Módulo de comunicaciones
SISTEMA DEL PROVEEDOR DE SERVICIOS DE PERSONALIZACIÓN (100)
Proveedor de servicios 1 (201)
Proveedor de servicios 2 (202)
Proveedor de servicios 3 (203)
Proveedor de servicios 4 (204)
Módulo de personalización de seguridad
BD asociada a aplicaciones software protegidas de dispositivo móvil
Aplicación software de dispositivo móvil
Software de protección de seguridad
RPS-I
RS1
RS2
RS3
RS4
RSi
RSn
RPS21
RPS31
RPS41
RPSi1
RPSn1
RPS22
RPS32
RPS42
RPSi2
RPSn2
RPS23
RPS33
RPS43
RPSi3
RPSn3
RPS2j
RPS3j
RPS4j
RPSij
RPSnj
RPS2N
RPS3N
RPS4N
RPSiN
RPSnN
(0)
(0')
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14a)
(14b)
(14c)
(14d)
(14e)
(15a)
(15b)
(15c)
(15d)
(15e)
(16a)
(16b)
(16c)
(16d)
(16e)
(17)
(18)
(19)

Figura 2.a

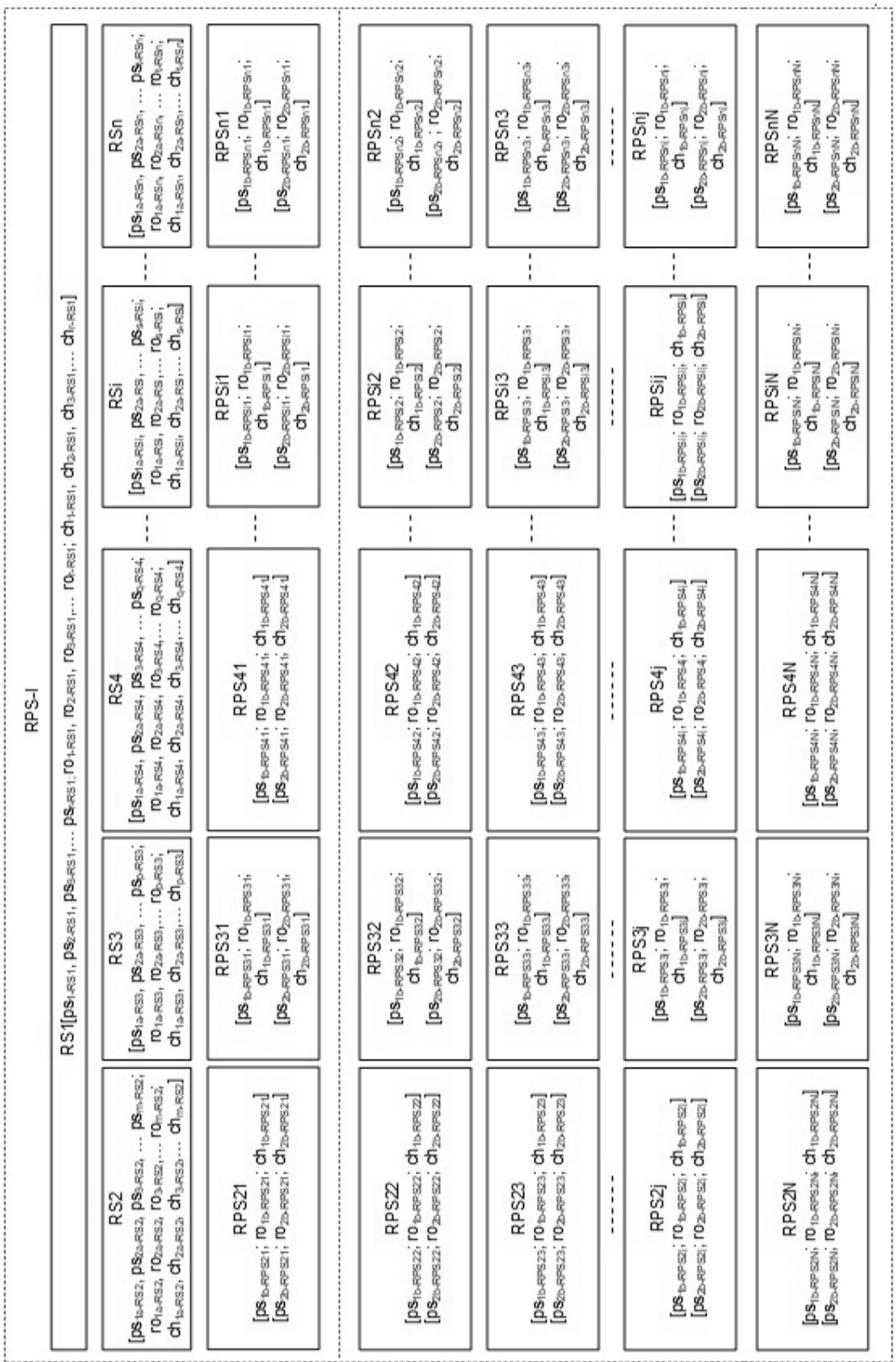

RPS-I
RS1
RS2
RS3
RS4
RSi
RSn
RPS21
RPS22
RPS2j
RPS2N
RPS31
RPS32
RPS3j
RPS3N
RPS41
RPS42
RPS4j
RPS4N
RPSi1
RPSi2
RPSij
RPSiN
RPSn1
RPSn2
RPSnj
RPSnN
RPS23
RPS33
RPS43
RPSi3
RPSn3

Figura 2.b

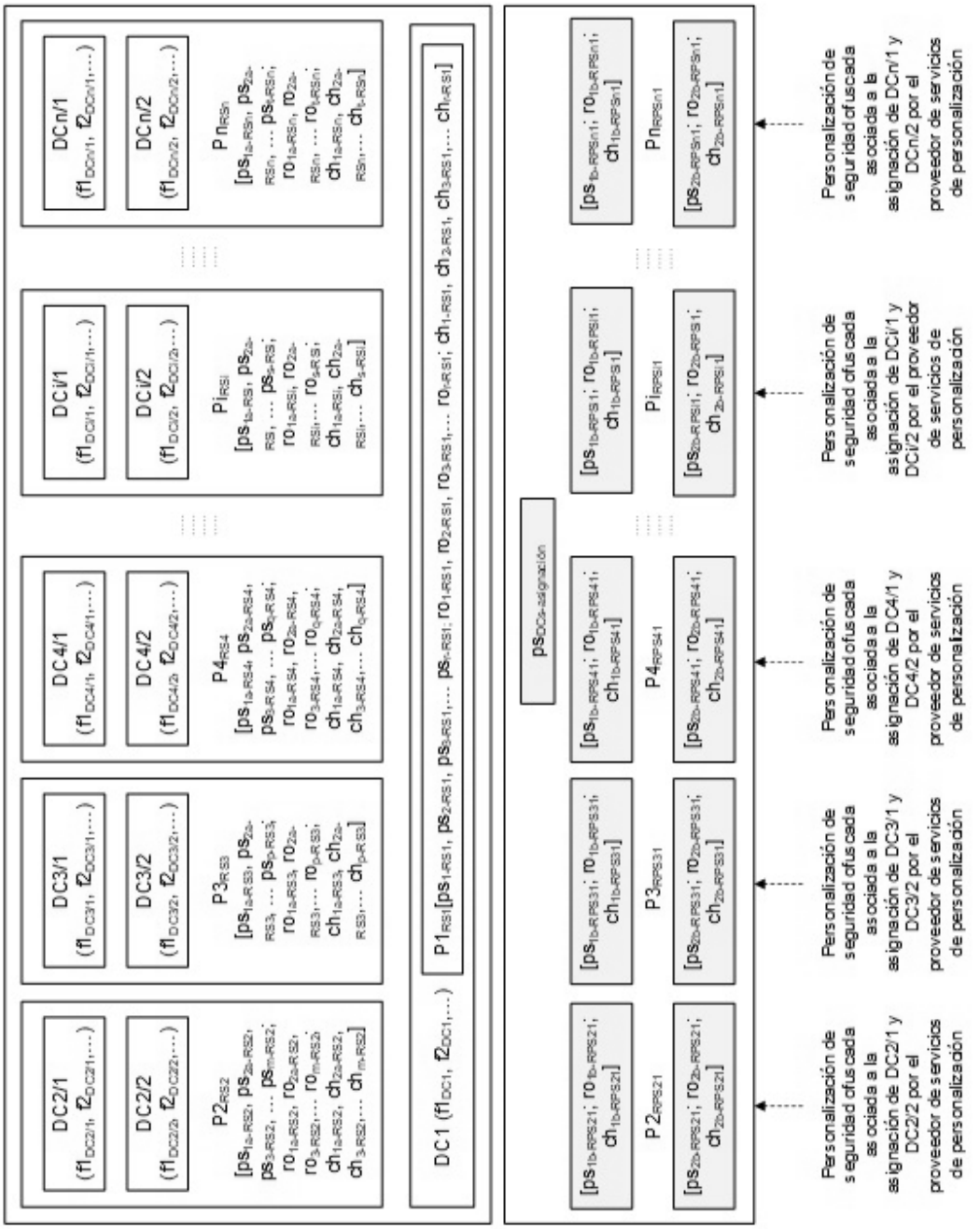
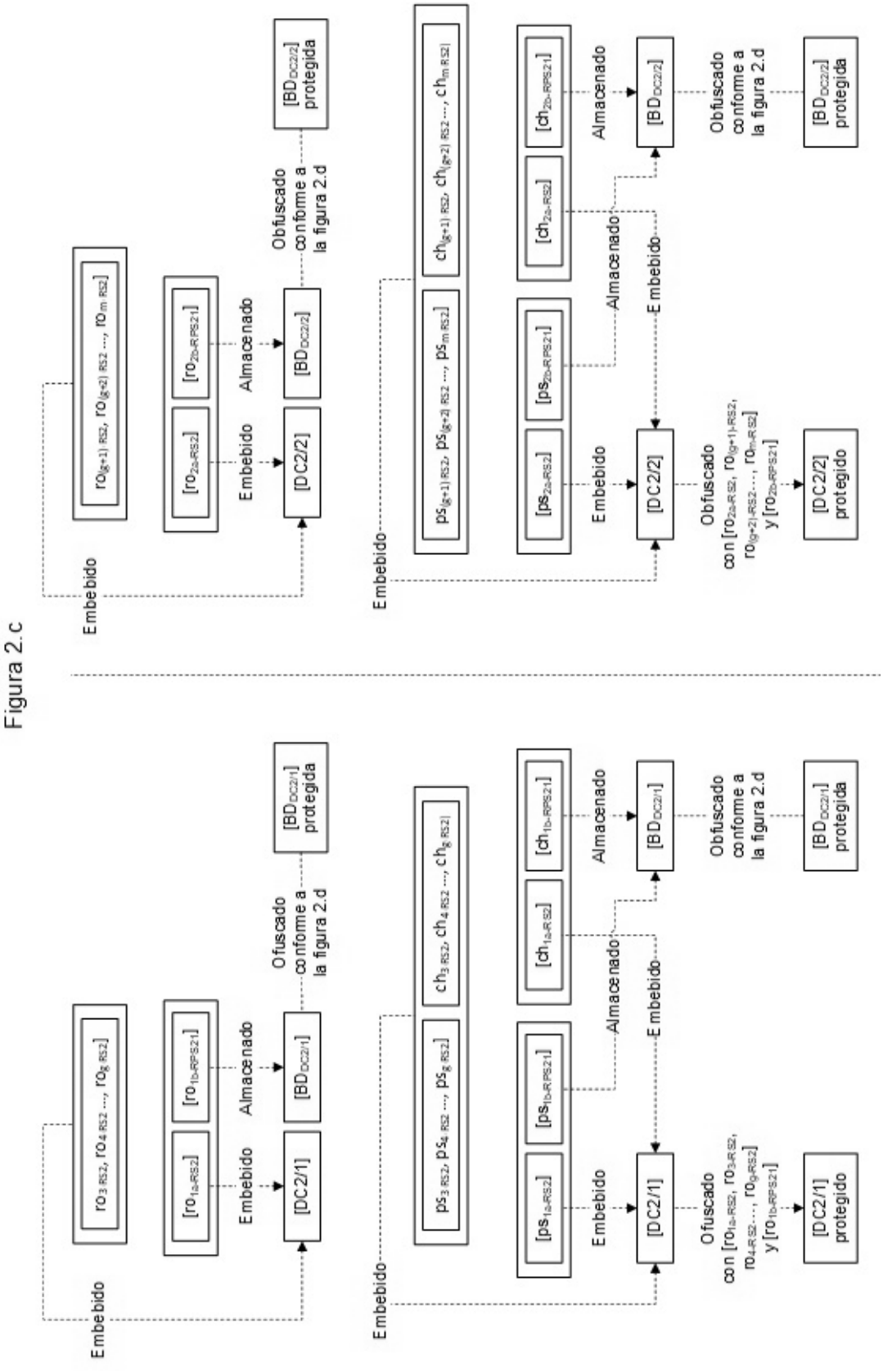

DC2/1 (f1DC2/1, f2DC2/1,...)
DC2/2 (f1DC2/2, f2DC2/2,...)
P2RS2 [psa-RS2, psb-RS2; psc-RS2; ro1a-RS2, ro2a-RS2; ro3-RS2,... rom-RS2; cha-RS2, chb-RS2,... chm-RS2]
DC3/1 (f1DC3/1, f2DC3/1,...)
DC3/2 (f1DC3/2, f2DC3/2,...)
P3RS3 [psa-RS3, psb-RS3; psc-RS3; ro1a-RS3, ro2a-RS3; ro3-RS3,... roq-RS3; cha-RS3, chb-RS3,... chq-RS3]
DC4/1 (f1DC4/1, f2DC4/1,...)
DC4/2 (f1DC4/2, f2DC4/2,...)
P4RS4 [psa-RS4, psb-RS4; psc-RS4; ro1a-RS4, ro2a-RS4; ro3-RS4,... roq-RS4; cha-RS4, chb-RS4,... chq-RS4]
DCi/1 (f1DCi/1, f2DCi/1,...)
DCi/2 (f1DCi/2, f2DCi/2,...)
Pi RSi [psa-RSi, psb-RSi; psc-RSi; ro1a-RSi, ro2a-RSi; ro3-RSi,... roq-RSi; cha-RSi, chb-RSi,... chq-RSi]
DCn/1 (f1DCn/1, f2DCn/1,...)
DCn/2 (f1DCn/2, f2DCn/2,...)
Pn RSn [psa-RSn, psb-RSn; psc-RSn; ro1a-RSn, ro2a-RSn; ro3-RSn,... roq-RSn; cha-RSn, chb-RSn,... chq-RSn]
DC1 (f1DC1, f2DC1,...)
P1RS1[psa-RS1, psb-RS1,... psk-RS1, ro1-RS1, ro2-RS1, ro3-RS1,... roi-RS1; ch1-RS1, ch2-RS1, ch3-RS1,... chi-RS1]
psDCs-asignación
[psa-RPS21; rob-RPS21; chb-RPS21]
[psb-RPS21; rob-RPS21; chb-RPS21]
P 2RPS21
[psa-RPS31; rob-RPS31; chb-RPS31]
[psb-RPS31; rob-RPS31; chb-RPS31]
P3RPS31
[psa-RPS41; rob-RPS41; chb-RPS41]
[psb-RPS41; rob-RPS41; chb-RPS41]
P4RPS41
[psa-RPSi1; rob-RPSi1; chb-RPSi1]
[psb-RPSi1; rob-RPSi1; chb-RPSi1]
Pi RPSi1
[psa-RPSn1; rob-RPSn1; chb-RPSn1]
[psb-RPSn1; rob-RPSn1; chb-RPSn1]
Pn RPSn1
Personalización de seguridad ofuscada asociada a la asignación de DC2/1 y DC2/2 por el proveedor de servicios de personalización
Personalización de seguridad ofuscada asociada a la asignación de DC3/1 y DC3/2 por el proveedor de servicios de personalización
Personalización de seguridad ofuscada asociada a la asignación de DC4/1 y DC4/2 por el proveedor de servicios de personalización
Personalización de seguridad ofuscada asociada a la asignación de DCi/1 y DCi/2 por el proveedor de servicios de personalización
Personalización de seguridad ofuscada asociada a la asignación de DCn/1 y DCn/2 por el proveedor de servicios de personalización

Figura 2.c


Embebido
Embebido
Almacenado
Obfuscado conforme a la figura 2.d
Embebido
Almacenado
Obfuscado conforme a la figura 2.d
Embebido
Embebido
Almacenado
Obfuscado con y
Embebido
Embebido
Almacenado
Obfuscado con y

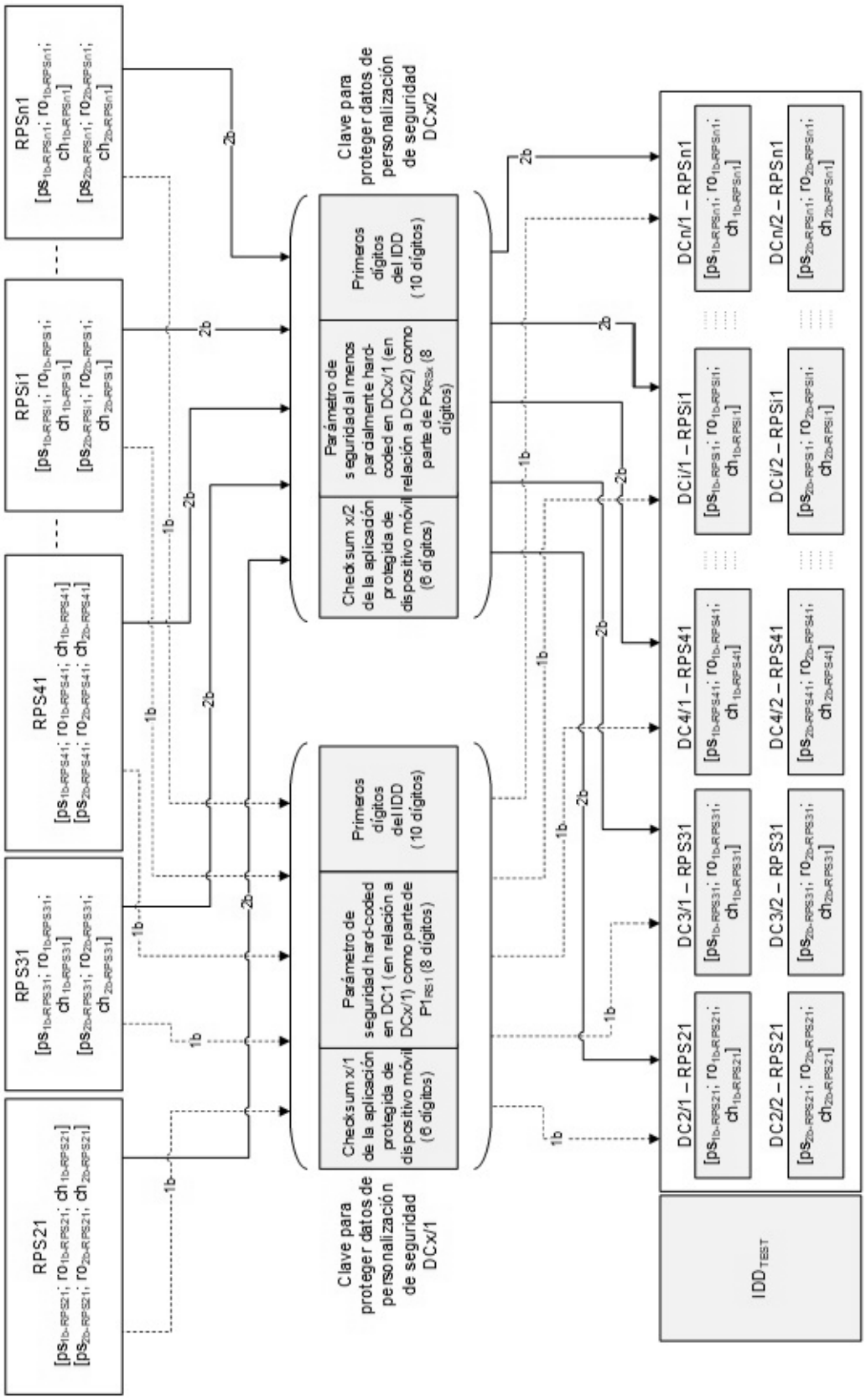

RPSn1
RPSi1
RPS41
RPS31
RPS21
Clave para proteger datos de personalización de seguridad DCx/2
Primeros dígitos del IDD (10 dígitos)
Parámetro de seguridad al menos parcialmente hard-coded en DCx/1 (en relación a DCx/2) como parte de PXRSx (8 dígitos)
Checksum x/2 de la aplicación protegida de dispositivo móvil (8 dígitos)
Clave para proteger datos de personalización de seguridad DCx/1
Primeros dígitos del IDD (10 dígitos)
Parámetro de seguridad hard-coded en DC1 (en relación a DCx/1) como parte de P1RS1 (8 dígitos)
Checksum x/1 de la aplicación protegida de dispositivo móvil (8 dígitos)
IDDTEST
DCn/1 – RPSn1
DCn/2 – RPSn1
DCi/1 – RPSi1
DCi/2 – RPSi1
DC4/1 – RPS41
DC4/2 – RPS41
DC3/1 – RPS31
DC3/2 – RPS31
DC2/1 – RPS21
DC2/2 – RPS21
1b
2b

Figura 2.d

Figura 2.e

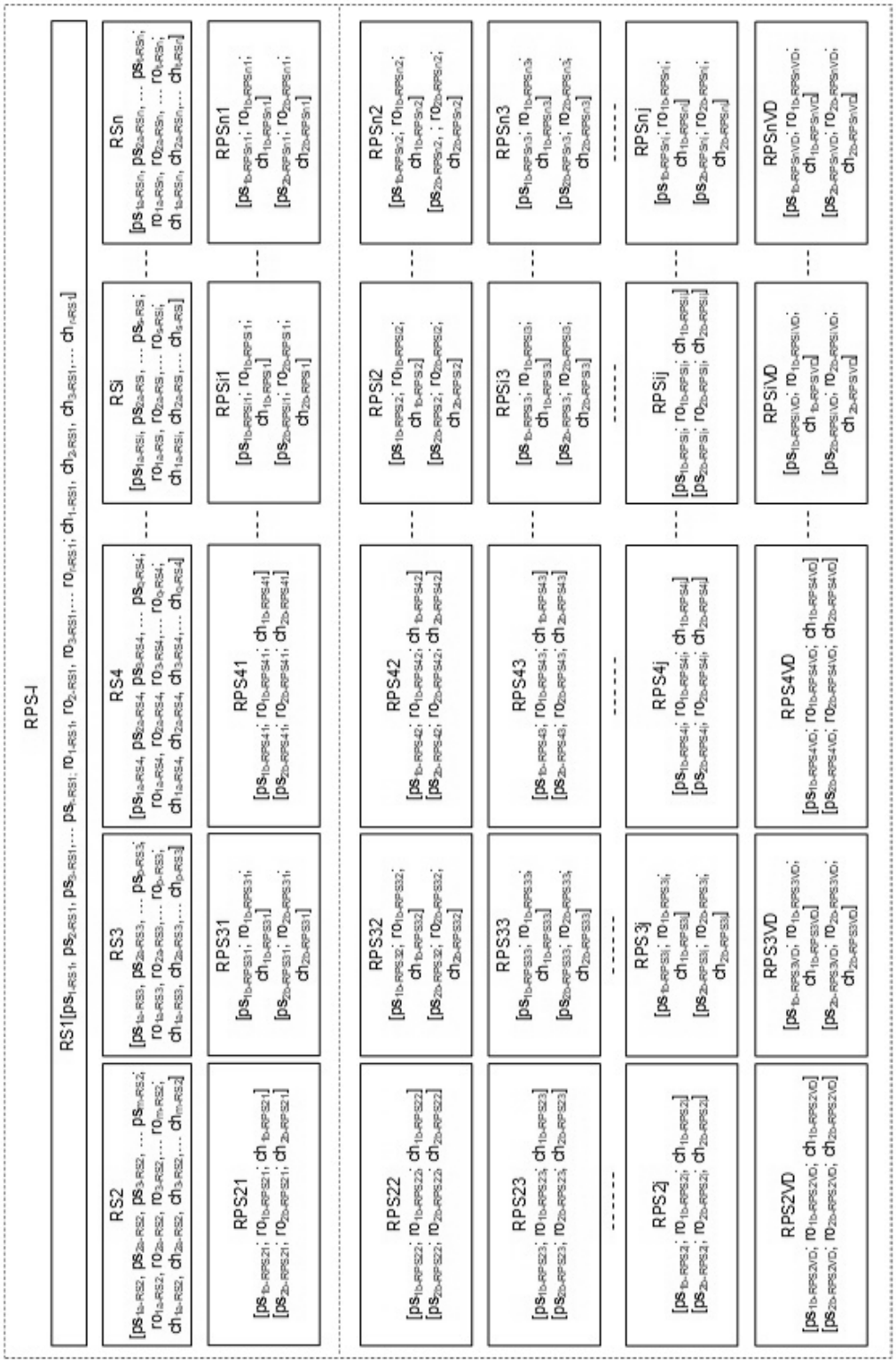
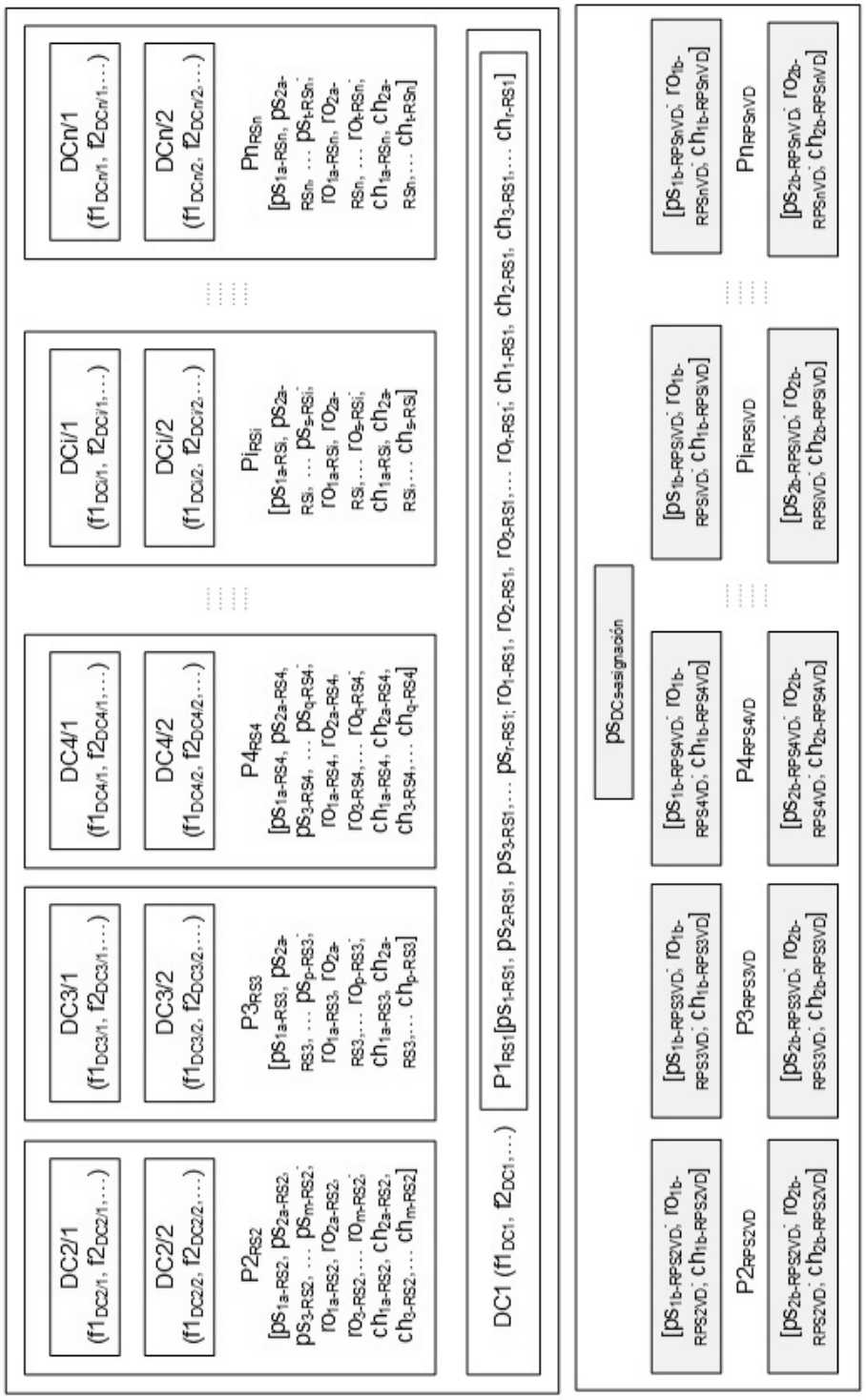

RPS-I
RS1
RS2
RS3
RS4
RSi
RSn
RPS21
RPS31
RPS41
RPSi1
RPSn1
RPS22
RPS32
RPS42
RPSi2
RPSn2
RPS23
RPS33
RPS43
RPSi3
RPSn3
RPS2j
RPS3j
RPS4j
RPSij
RPSnj
RPS2VD
RPS3VD
RPS4VD
RPSiVD
RPSnVD

Figura 2.f


DC2/1 (f1DC2/1, f2DC2/1,...)
DC2/2 (f1DC2/2, f2DC2/2,...)
P2RS2 [psRS2, ... psRS2, roRS2, ... roRS2, chRS2, ... chRS2]
DC3/1 (f1DC3/1, f2DC3/1,...)
DC3/2 (f1DC3/2, f2DC3/2,...)
P3RS3 [psRS3, ... psRS3, roRS3, ... roRS3, chRS3, ... chRS3]
DC4/1 (f1DC4/1, f2DC4/1,...)
DC4/2 (f1DC4/2, f2DC4/2,...)
P4RS4 [psRS4, ... psRS4, roRS4, ... roRS4, chRS4, ... chRS4]
DCi/1 (f1DCi/1, f2DCi/1,...)
DCi/2 (f1DCi/2, f2DCi/2,...)
PiRSi [psRSi, ... psRSi, roRSi, ... roRSi, chRSi, ... chRSi]
DCn/1 (f1DCn/1, f2DCn/1,...)
DCn/2 (f1DCn/2, f2DCn/2,...)
PnRSn [psRSn, ... psRSn, roRSn, ... roRSn, chRSn, ... chRSn]
DC1 (f1DC1, f2DC1,...)
P1RS1[psRS1, psRS1, psRS1,... psRS1; roRS1, roRS1, roRS1,... roRS1; chRS1, chRS1, chRS1,... chRS1]
psDCasignación
[psRPS2VD; roRPS2VD; chRPS2VD]
[psRPS2VD; roRPS2VD; chRPS2VD]
P2RPS2VD
[psRPS3VD; roRPS3VD; chRPS3VD]
[psRPS3VD; roRPS3VD; chRPS3VD]
P3RPS3VD
[psRPS4VD; roRPS4VD; chRPS4VD]
[psRPS4VD; roRPS4VD; chRPS4VD]
P4RPS4VD
[psRPSiVD; roRPSiVD; chRPSiVD]
[psRPSiVD; roRPSiVD; chRPSiVD]
PiRPSiVD
[psRPSnVD; roRPSnVD; chRPSnVD]
[psRPSnVD; roRPSnVD; chRPSnVD]
PnRPSnVD

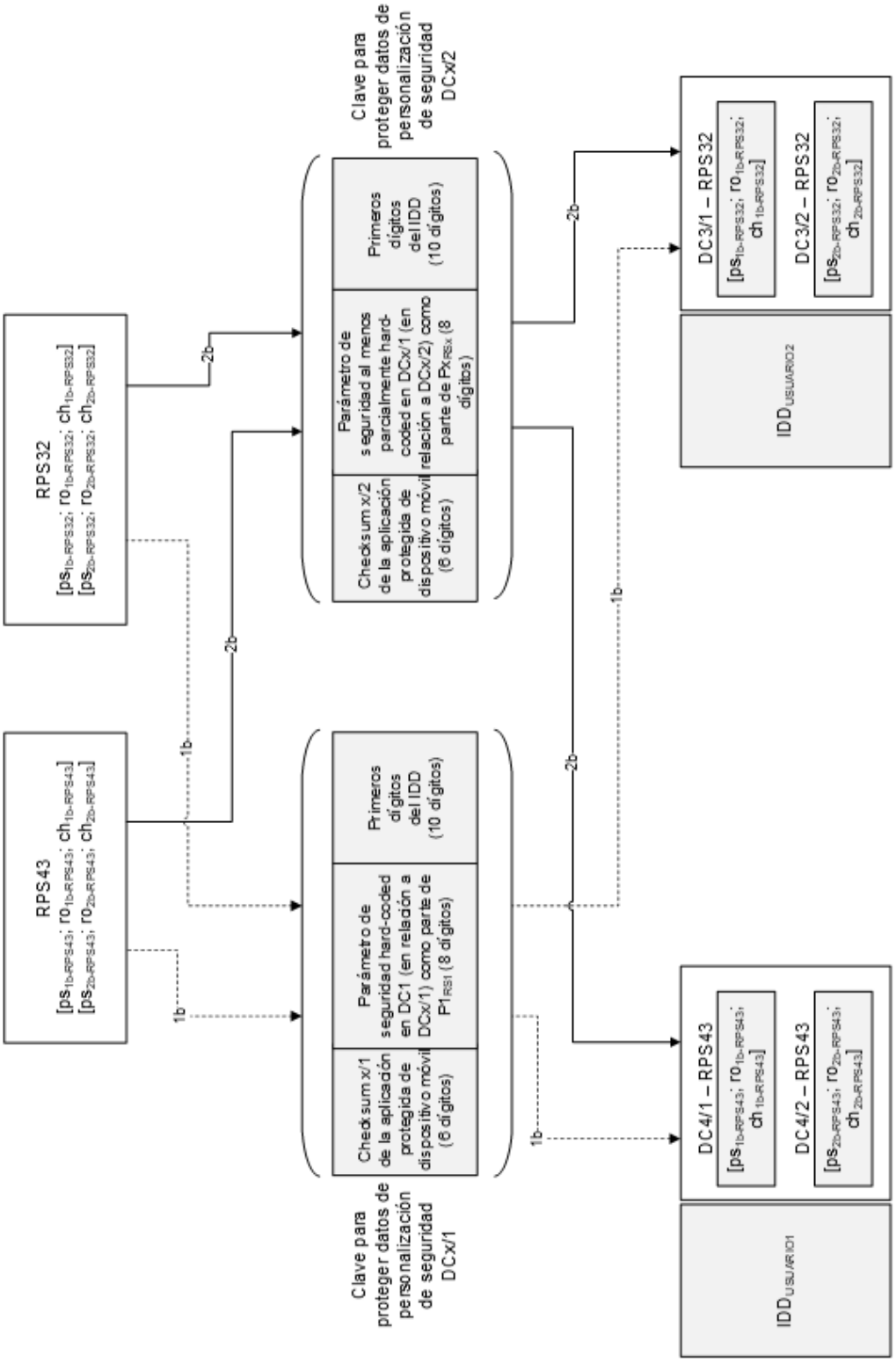

RPS43
[ps1b-RPS43; ro1b-RPS43; ch1b-RPS43]
[ps2b-RPS43; ro2b-RPS43; ch2b-RPS43]
RPS32
[ps1b-RPS32; ro1b-RPS32; ch1b-RPS32]
[ps2b-RPS32; ro2b-RPS32; ch2b-RPS32]
1b
2b
Checksum x/1 de la aplicación protegida de dispositivo móvil (6 dígitos)
Parámetro de seguridad hard-coded en DC1 (en relación a DCx/1) como parte de P1RS1 (8 dígitos)
Primeros dígitos del IDD (10 dígitos)
Clave para proteger datos de personalización de seguridad DCx/1
Checksum x/2 de la aplicación protegida de dispositivo móvil (6 dígitos)
Parámetro de seguridad al menos parcialmente hard-coded en DCx/1 (en relación a DCx/2) como parte de PxRSx (8 dígitos)
Primeros dígitos del IDD (10 dígitos)
Clave para proteger datos de personalización de seguridad DCx/2
DC4/1 – RPS43
[ps1b-RPS43; ro1b-RPS43; ch1b-RPS43]
DC4/2 – RPS43
[ps2b-RPS43; ro2b-RPS43; ch2b-RPS43]
IDDUSUARIO1
DC3/1 – RPS32
[ps1b-RPS32; ro1b-RPS32; ch1b-RPS32]
DC3/2 – RPS32
[ps2b-RPS32; ro2b-RPS32; ch2b-RPS32]
IDDUSUARIO2

Figura 2.g

DC2/1 (f1DC2/1, f2DC2/1,...)
DC2/2 (f1DC2/2, f2DC2/2,...)
P2 [psRS2, ... psRS2; roRS2, ... roRS2; chRS2, ... chRS2]
DC3/1 (f1DC3/1, f2DC3/1,...)
DC3/2 (f1DC3/2, f2DC3/2,...)
P3 [psRS3, ... psRS3; roRS3, ... roRS3; chRS3, ... chRS3]
DC4/1 (f1DC4/1, f2DC4/1,...)
DC4/2 (f1DC4/2, f2DC4/2,...)
P4 [psRS4, ... psRS4; roRS4, ... roRS4; chRS4, ... chRS4]
DCi/1 (f1DCi/1, f2DCi/1,...)
DCi/2 (f1DCi/2, f2DCi/2,...)
Pi [psRSi, ... psRSi; roRSi, ... roRSi; chRSi, ... chRSi]
DCn/1 (f1DCn/1, f2DCn/1,...)
DCn/2 (f1DCn/2, f2DCn/2,...)
Pn [psRSn, ... psRSn; roRSn, ... roRSn; chRSn, ... chRSn]
DC1 (f1DC1, f2DC1,...)
P1RS1[psRS1, psRS1, ... psRS1; roRS1, roRS1, ... roRS1; chRS1, chRS1, ... chRS1]
psDCs=asignación
[psRPS2VD; roRPS2VD; chRPS2VD]
[psRPS2VD; roRPS2VD; chRPS2VD]
[psRPS3VD; roRPS3VD; chRPS3VD]
[psRPS3VD; roRPS3VD; chRPS3VD]
[psRPS43; roRPS43; chRPS43]
[psRPS4VD; roRPS4VD; chRPS4VD]
[psRPS4VD; roRPS4VD; chRPS4VD]
[psRPSiVD; roRPSiVD; chRPSiVD]
[psRPSiVD; roRPSiVD; chRPSiVD]
[psRPSnVD; roRPSnVD; chRPSnVD]
[psRPSnVD; roRPSnVD; chRPSnVD]

Figura 2.h

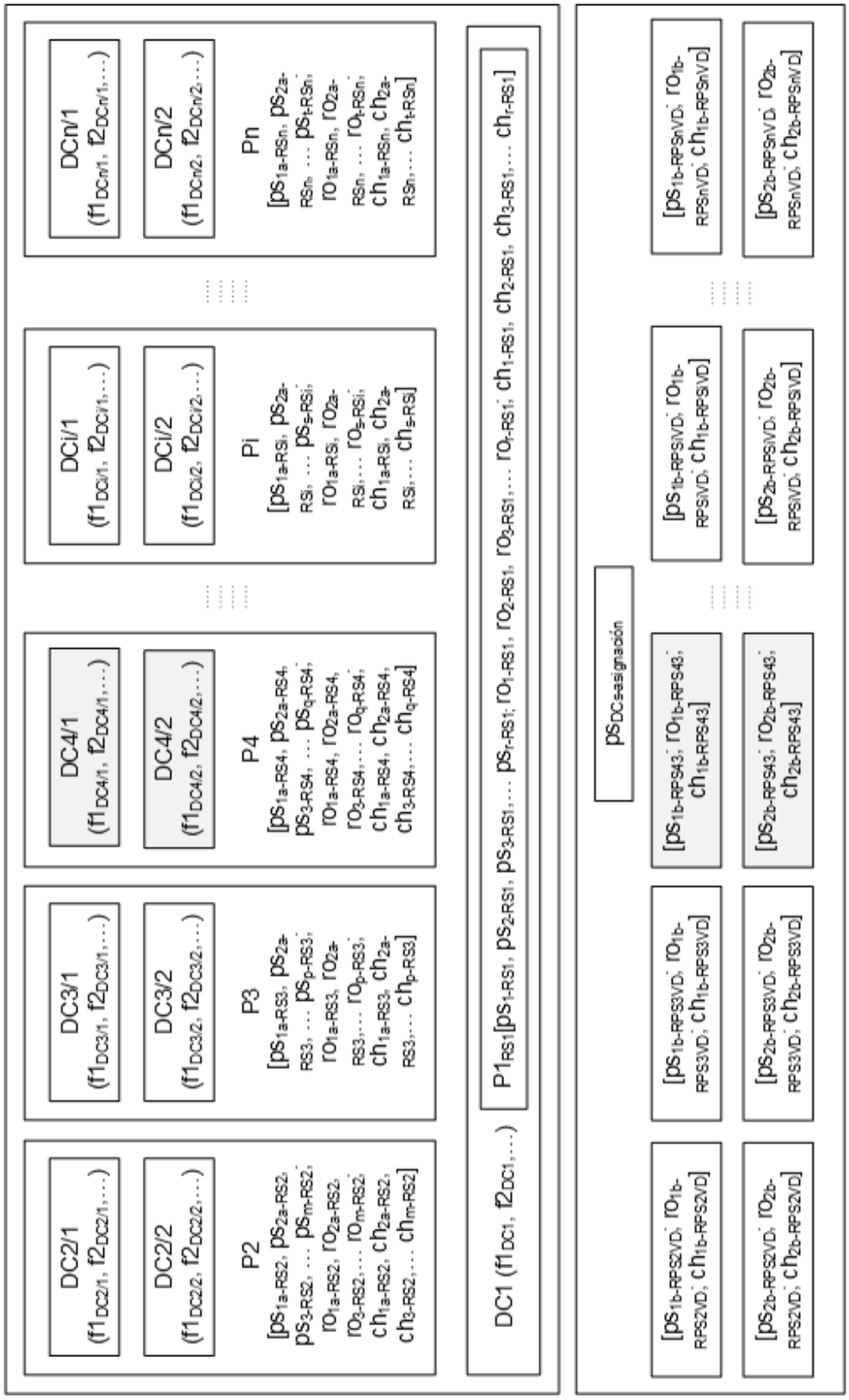

DC2/1 (f1DC2/1, f2DC2/1,...)
DC2/2 (f1DC2/2, f2DC2/2,...)
P2 [ps1a-RS2, ps2a-RS2, ps3-RS2, ... psm-RS2; ro1a-RS2, ro2a-RS2, ro3-RS2,... rom-RS2; ch1a-RS2, ch2a-RS2, ch3-RS2,... chm-RS2]
DC3/1 (f1DC3/1, f2DC3/1,...)
DC3/2 (f1DC3/2, f2DC3/2,...)
P3 [ps1a-RS3, ps2a-RS3, ... psp-RS3; ro1a-RS3, ro2a-RS3,... rop-RS3; ch1a-RS3, ch2a-RS3,... chp-RS3]
DC4/1 (f1DC4/1, f2DC4/1,...)
DC4/2 (f1DC4/2, f2DC4/2,...)
P4 [ps1a-RS4, ps2a-RS4, ps3-RS4, ... psq-RS4; ro1a-RS4, ro2a-RS4, ro3-RS4,... roq-RS4; ch1a-RS4, ch2a-RS4, ch3-RS4,... chq-RS4]
DCi/1 (f1DCi/1, f2DCi/1,...)
DCi/2 (f1DCi/2, f2DCi/2,...)
Pi [ps1a-RSi, ps2a-RSi, ... pss-RSi; ro1a-RSi, ro2a-RSi,... ros-RSi; ch1a-RSi, ch2a-RSi,... chs-RSi]
DCn/1 (f1DCn/1, f2DCn/1,...)
DCn/2 (f1DCn/2, f2DCn/2,...)
Pn [ps1a-RSn, ps2a-RSn, ... pst-RSn; ro1a-RSn, ro2a-RSn,... rot-RSn; ch1a-RSn, ch2a-RSn,... cht-RSn]
DC1 (f1DC1, f2DC1,...)
P1RS1[ps1-RS1, ps2-RS1, ps3-RS1,... psr-RS1; ro1-RS1, ro2-RS1, ro3-RS1,... ror-RS1; ch1-RS1, ch2-RS1, ch3-RS1,... chr-RS1]
psDC=asignación
[ps1b-RPS2VD; ro1b-RPS2VD; ch1b-RPS2VD]
[ps2b-RPS2VD; ro2b-RPS2VD; ch2b-RPS2VD]
[ps1b-RPS3VD; ro1b-RPS3VD; ch1b-RPS3VD]
[ps2b-RPS3VD; ro2b-RPS3VD; ch2b-RPS3VD]
[ps1b-RPS43; ro1b-RPS43; ch1b-RPS43]
[ps2b-RPS43; ro2b-RPS43; ch2b-RPS43]
[ps1b-RPSiVD; ro1b-RPSiVD; ch1b-RPSiVD]
[ps2b-RPSiVD; ro2b-RPSiVD; ch2b-RPSiVD]
[ps1b-RPSnVD; ro1b-RPSnVD; ch1b-RPSnVD]
[ps2b-RPSnVD; ro2b-RPSnVD; ch2b-RPSnVD]

Figura 2.i

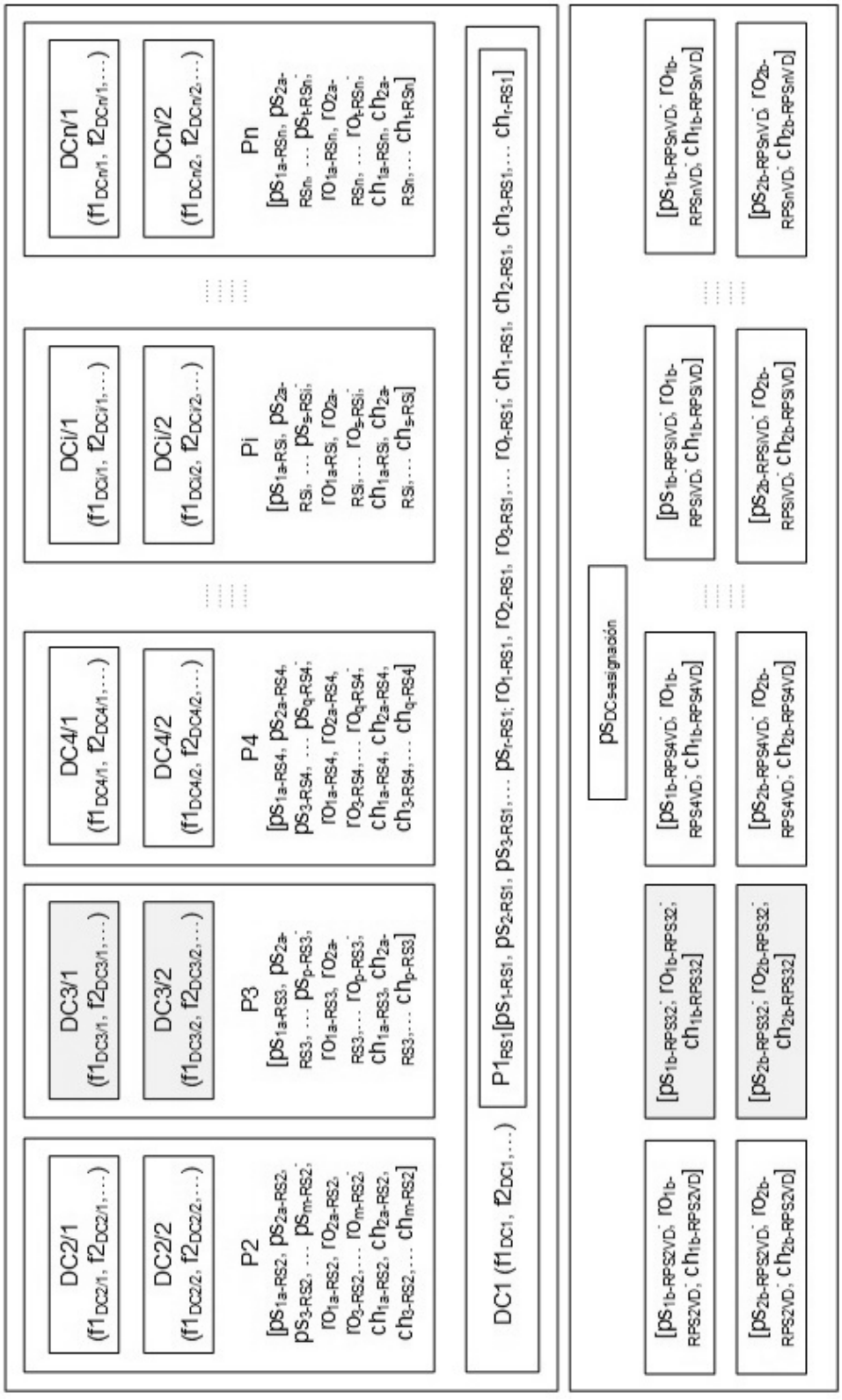

DC1 (f1DC1, f2DC1,....)
P1RS1[psT-RS1, psZ-RS1, psS-RS1,.... psR-RS1; rO1-RS1, rO2-RS1, rO3-RS1,.... rOT-RS1; ch1-RS1, ch2-RS1, ch3-RS1,.... chT-RS1]
DC2/1 (f1DC2/1, f2DC2/1,....)
DC2/2 (f1DC2/2, f2DC2/2,....)
P2 [psU-RS2, psZ-RS2, psS-RS2,.... psM-RS2; rO1a-RS2, rO2a-RS2, rO3-RS2,.... rOm-RS2; ch1a-RS2, ch2a-RS2, ch3-RS2,.... chm-RS2]
DC3/1 (f1DC3/1, f2DC3/1,....)
DC3/2 (f1DC3/2, f2DC3/2,....)
P3 [psU-RS3, psZ-RS3, psP-RS3; rO1a-RS3, rO2a-RS3,.... rOp-RS3; ch1a-RS3, ch2a-RS3, ch3-RS3,.... chp-RS3]
DC4/1 (f1DC4/1, f2DC4/1,....)
DC4/2 (f1DC4/2, f2DC4/2,....)
P4 [psU-RS4, psZ-RS4, psS-RS4, ... psQ-RS4; rO1a-RS4, rO2a-RS4, rO3-RS4,.... rOq-RS4; ch1a-RS4, ch2a-RS4, ch3-RS4,.... chq-RS4]
DCi/1 (f1DCi/1, f2DCi/1,....)
DCi/2 (f1DCi/2, f2DCi/2,....)
Pi [psU-RSi, psZ-RSi, psS-RSi; rO1a-RSi, rO2a-RSi,.... rOs-RSi; ch1a-RSi, ch2a-RSi,.... chs-RSi]
DCn/1 (f1DCn/1, f2DCn/1,....)
DCn/2 (f1DCn/2, f2DCn/2,....)
Pn [psU-RSn, psZ-RSn, psS-RSn; rO1a-RSn, rO2a-RSn,.... rOt-RSn; ch1a-RSn, ch2a-RSn,.... chT-RSn]
psDCs=asignación
[psU-RPS2VD; rO1b-RPS2VD; ch1b-RPS2VD]
[psZ-RPS2VD; rO2b-RPS2VD; ch2b-RPS2VD]
[psU-RPS32; rO1b-RPS32; ch1b-RPS32]
[psZ-RPS32; rO2b-RPS32; ch2b-RPS32]
[psU-RPS4VD; rO1b-RPS4VD; ch1b-RPS4VD]
[psZ-RPS4VD; rO2b-RPS4VD; ch2b-RPS4VD]
[psU-RPSiVD; rO1b-RPSiVD; ch1b-RPSiVD]
[psZ-RPSiVD; rO2b-RPSiVD; ch2b-RPSiVD]
[psU-RPSnVD; rO1b-RPSnVD; ch1b-RPSnVD]
[psZ-RPSnVD; rO2b-RPSnVD; ch2b-RPSnVD]

Figura 2.j

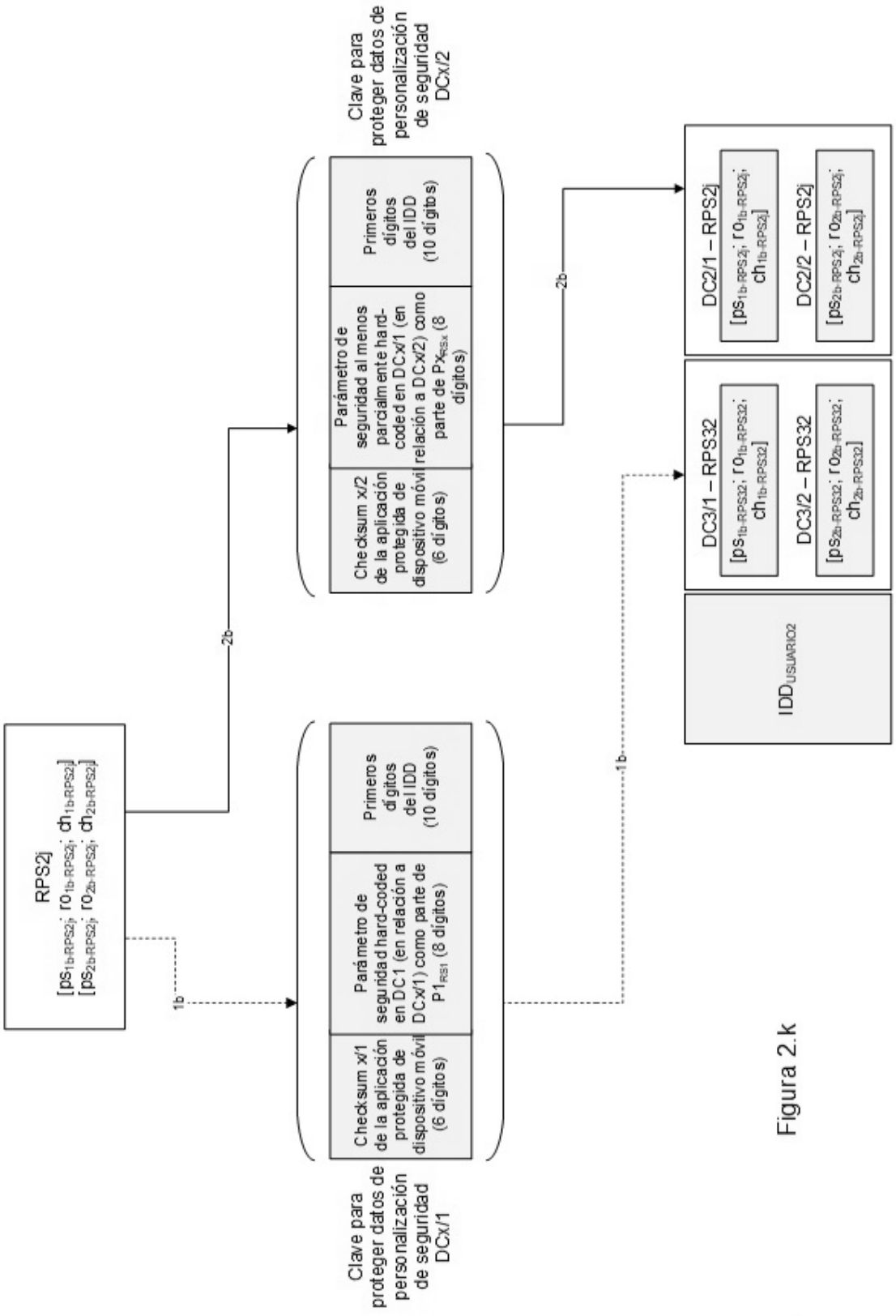

RPS2j
[ps1b-RPS2j; ro1b-RPS2j; ch1b-RPS2j]
[ps2b-RPS2j; ro2b-RPS2j; ch2b-RPS2j]
1b
2b
Checksum x/1 de la aplicación protegida de dispositivo móvil (6 dígitos)
Parámetro de seguridad hard-coded en DC1 (en relación a DCx/1) como parte de P1RS1 (8 dígitos)
Primeros dígitos del IDD (10 dígitos)
Clave para proteger datos de personalización de seguridad DCx/1
Checksum x/2 de la aplicación protegida de dispositivo móvil (6 dígitos)
Parámetro de seguridad al menos parcialmente hard-coded en DCx/1 (en relación a DCx/2) como parte de PxRSx (8 dígitos)
Primeros dígitos del IDD (10 dígitos)
Clave para proteger datos de personalización de seguridad DCx/2
IDDUSUARIO2
DC3/1 – RPS32
[ps1b-RPS32; ro1b-RPS32; ch1b-RPS32]
DC3/2 – RPS32
[ps2b-RPS32; ro2b-RPS32; ch2b-RPS32]
DC2/1 – RPS2j
[ps1b-RPS2j; ro1b-RPS2j; ch1b-RPS2j]
DC2/2 – RPS2j
[ps2b-RPS2j; ro2b-RPS2j; ch2b-RPS2j]

Figura 2.k

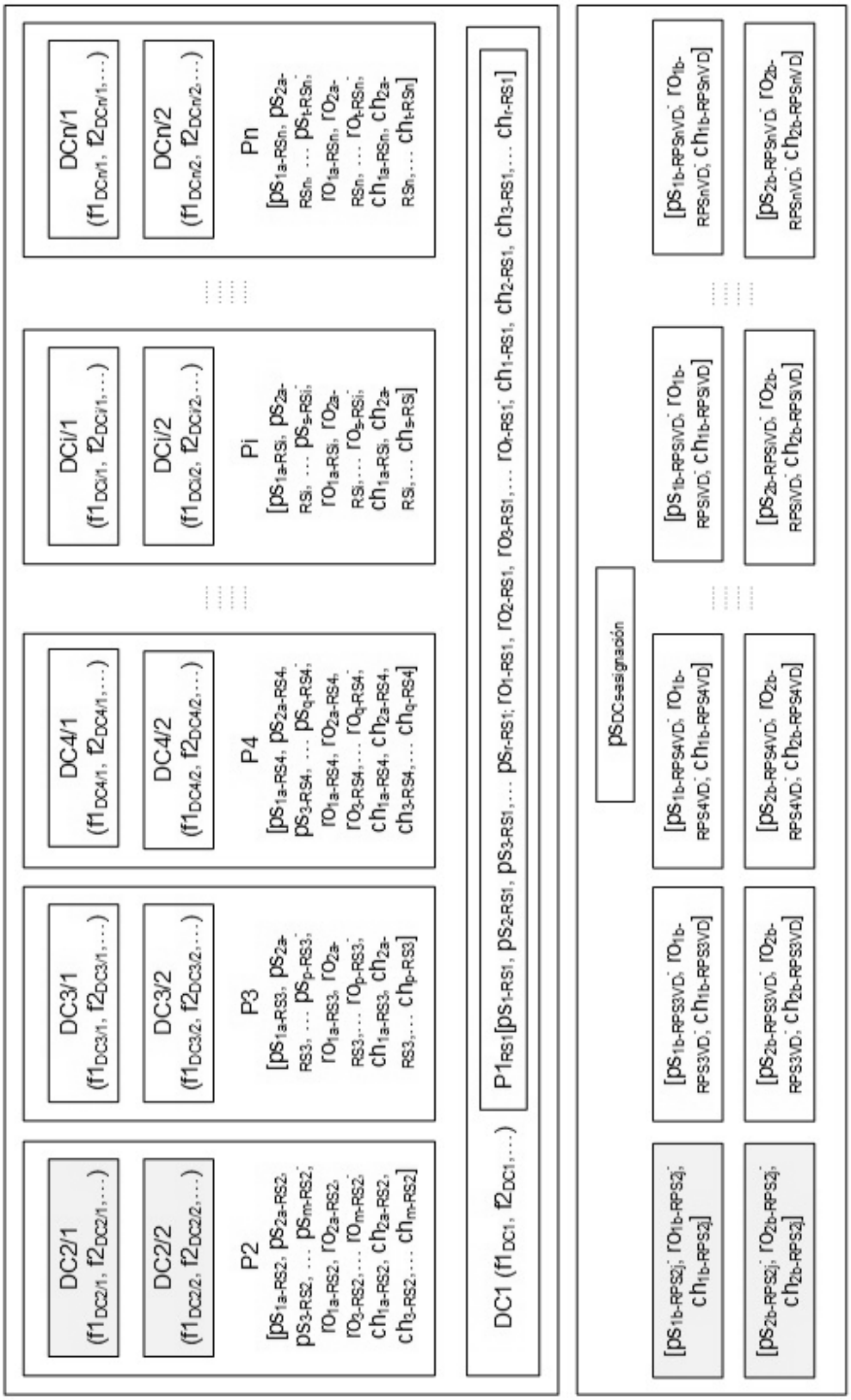

DC2/1 (f1DC2/1, f2DC2/1,...)
DC2/2 (f1DC2/2, f2DC2/2,...)
P2 [ps1a-RS2, ps2a-RS2, ps3-RS2, ... psm-RS2; ro1a-RS2, ro2a-RS2, ro3-RS2,... rom-RS2; ch1a-RS2, ch2a-RS2, ch3-RS2,... chm-RS2]
DC3/1 (f1DC3/1, f2DC3/1,...)
DC3/2 (f1DC3/2, f2DC3/2,...)
P3 [ps1a-RS3, ps2a-RS3, ... psp-RS3; ro1a-RS3, ro2a-RS3,... rop-RS3; ch1a-RS3, ch2a-RS3,... chp-RS3]
DC4/1 (f1DC4/1, f2DC4/1,...)
DC4/2 (f1DC4/2, f2DC4/2,...)
P4 [ps1a-RS4, ps2a-RS4, ps3-RS4, ... psq-RS4; ro1a-RS4, ro2a-RS4, ro3-RS4,... roq-RS4; ch1a-RS4, ch2a-RS4, ch3-RS4,... chq-RS4]
DCi/1 (f1DCi/1, f2DCi/1,...)
DCi/2 (f1DCi/2, f2DCi/2,...)
Pi [ps1a-RSi, ps2a-RSi, ... pss-RSi; ro1a-RSi, ro2a-RSi,... ros-RSi; ch1a-RSi, ch2a-RSi,... chs-RSi]
DCn/1 (f1DCn/1, f2DCn/1,...)
DCn/2 (f1DCn/2, f2DCn/2,...)
Pn [ps1a-RSn, ps2a-RSn, ... pst-RSn; ro1a-RSn, ro2a-RSn, ... rot-RSn; ch1a-RSn, ch2a-RSn,... chr-RSn]
DC1 (f1DC1, f2DC1,...)
P1RS1[ps1-RS1, ps2-RS1, ps3-RS1,... psr-RS1; ro1-RS1, ro2-RS1, ro3-RS1,... ror-RS1; ch1-RS1, ch2-RS1, ch3-RS1,... chr-RS1]
psDC=asignación
[ps1b-RPS2j; ro1b-RPS2j; ch1b-RPS2j]
[ps2b-RPS2j; ro2b-RPS2j; ch2b-RPS2j]
[ps1b-RPS3VD; ro1b-RPS3VD; ch1b-RPS3VD]
[ps2b-RPS3VD; ro2b-RPS3VD; ch2b-RPS3VD]
[ps1b-RPS4VD; ro1b-RPS4VD; ch1b-RPS4VD]
[ps2b-RPS4VD; ro2b-RPS4VD; ch2b-RPS4VD]
[ps1b-RPSiVD; ro1b-RPSiVD; ch1b-RPSiVD]
[ps2b-RPSiVD; ro2b-RPSiVD; ch2b-RPSiVD]
[ps1b-RPSnVD; ro1b-RPSnVD; ch1b-RPSnVD]
[ps2b-RPSnVD; ro2b-RPSnVD; ch2b-RPSnVD]

Figura 2.I

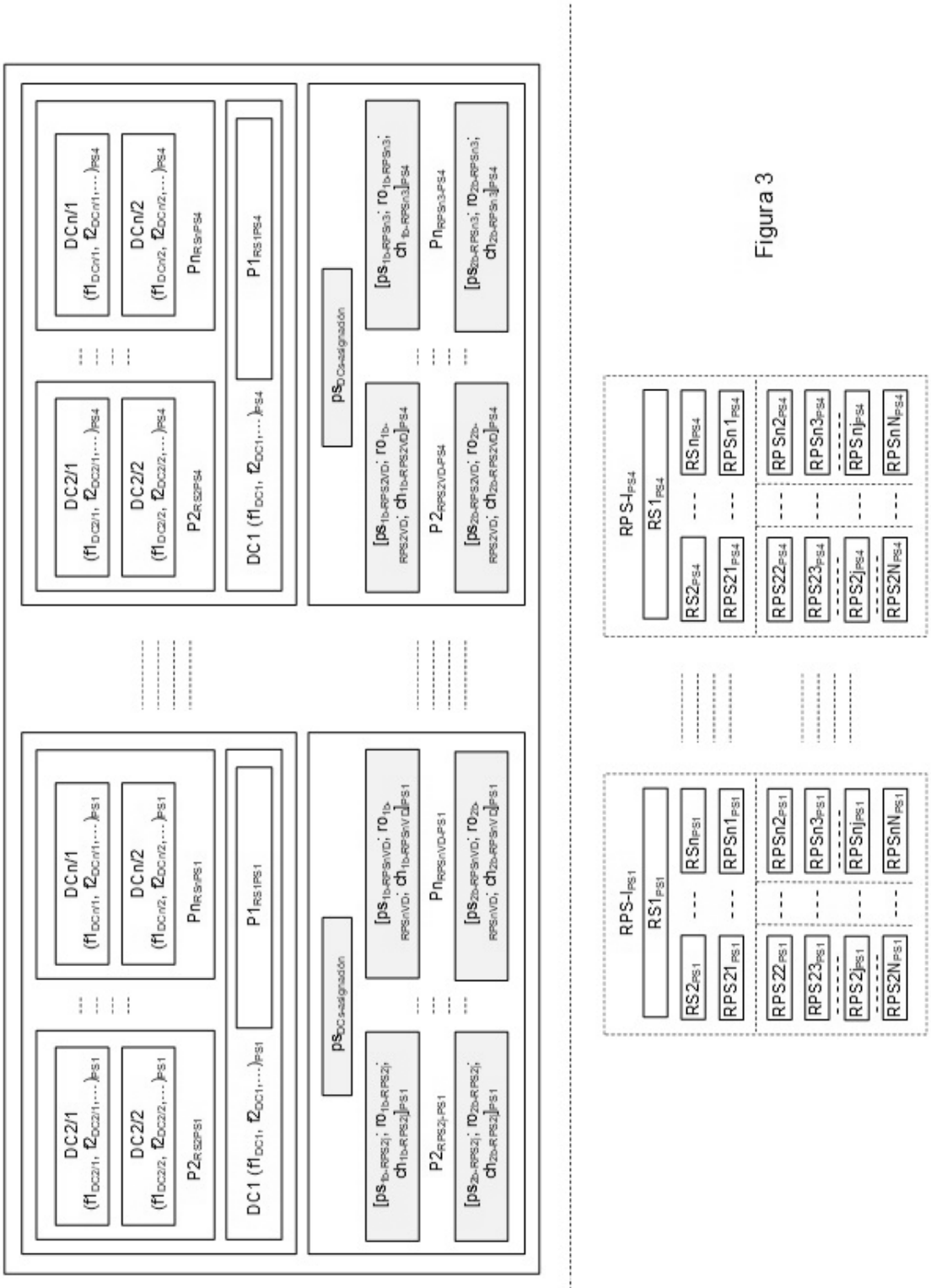

DC2/1
DC2/2
P2RS2PS1
DC1
P1RS1PS1
DCn/1
DCn/2
PnRSnPS1
psDCs-asignados
P2RPS2jPS1
PnRPSnVDPS1
RPS-IPS1
RS1PS1
RS2PS1
RPS21PS1
RPS22PS1
RPS23PS1
RPS2jPS1
RPS2NPS1
RSnPS1
RPSn1PS1
RPSn2PS1
RPSn3PS1
RPSnjPS1
RPSnNPS1
DC2/1
DC2/2
P2RS2PS4
DC1
P1RS1PS4
DCn/1
DCn/2
PnRSnPS4
psDCs-asignados
P2RPS2VDPS4
PnRPSn3PS4
RPS-IPS4
RS1PS4
RS2PS4
RPS21PS4
RPS22PS4
RPS23PS4
RPS2jPS4
RPS2NPS4
RSnPS4
RPSn1PS4
RPSn2PS4
RPSn3PS4
RPSnjPS4
RPSnNPS4

Figura 3