(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 607 495**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.12.2014 E 14199297 (4)**

(97) Fecha y número de publicación de la concesión europea: **26.10.2016 EP 2894891**

(54) Título: **Testigo móvil**

(30) Prioridad:

20.12.2013 US 201361919230 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.03.2017

(73) Titular/es:

VERISEC AB (100.0%)
P.O. Box 2034
131 02 Nacka, SE

(72) Inventor/es:

NESIC, DRAGOLJUB

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Testigo móvil

Campo de la invención

La presente invención se refiere a un método para establecer un secreto compartido entre un primer y un segundo dispositivo sin ninguna confianza compartida entre el primer y segundo dispositivo, para el uso de servicios proporcionados por un proveedor de servicios a un usuario de dicho segundo dispositivo.

La presente invención también se refiere a un sistema adaptado para establecer un secreto compartido de acuerdo con el método inventivo.

La presente invención también se refiere a productos de programa informático a través de los cuales pueden realizarse los métodos inventivos y a un medio legible por ordenador que lleva un producto de programa informático inventivo.

Descripción de los antecedentes de la técnica

Es conocido usar autenticación de dos factores y contraseñas de un solo uso para proteger servicios de acceso proporcionados por los proveedores de servicio de una manera segura, donde los usuarios normalmente usan contraseñas fijas, a menudo seleccionadas de modo que son fáciles de recordar.

Los proveedores de servicios, de aplicaciones web o en la nube y redes corporativas requieren un sistema basado en norma abierta que no les bloquee a trabajar con una tecnología y proveedor propietarios, pero que proporcione una amplia diversidad de dispositivos de autenticación, basados tanto en hardware como software, autenticadores móviles, SMS OTP y más.

Los usuarios cada vez acceden más a aplicaciones que se ejecutan en la nube y los proveedores desean mantener el control de la autenticación de estas aplicaciones.

Es necesario que se aprovisione a los que entran con cuentas de usuario y contraseñas para las aplicaciones en la nube, y es necesario que se interrumpa el acceso a los que abandonan esas mismas aplicaciones.

Puede mencionarse también que existe un algoritmo conocido para autenticación de desafío-respuesta desarrollado por la Iniciativa para la Autenticación Abierta (OATH) denominado OCRA: Algoritmo de Desafío-Respuesta de OATH.

La publicación de patente US 2011/0197266 A1 muestra que los métodos y sistemas para autenticación de usuario segura que usan un OTP implican, por ejemplo, pre-almacenar una aplicación de OTP en un primer dispositivo informático para generar un valor de OTP válido para el usuario en respuesta a recibir entrada de un valor de PIN válido del usuario, no se almacena parte del valor de PIN válido en el primer dispositivo informático y pre-almacenar en un servidor de extremo trasero el valor de PIN válido y un secreto compartido válido para el usuario. Tras recibir la entrada de un valor de PIN pretendido del usuario, se sintetiza dinámicamente un secreto compartido pretendido en el primer dispositivo informático mediante la aplicación de OTP basándose en el valor de PIN pretendido del usuario y se genera un valor de OTP pretendido en el primer dispositivo informático. Cuando se recibe la entrada del valor de OTP pretendido mediante el servidor de extremo trasero en un intento para registrarse en el servidor de extremo trasero desde un segundo dispositivo informático, el servidor de extremo trasero calcula criptográficamente una ventana de valores de OTP, y se permite el inicio de sesión en el servidor de extremo trasero desde el segundo dispositivo informático si la ventana calculada de valores de OTP corresponde al valor de OTP recibido.

Sumario de la presente invención

Problemas

El uso de autenticación de dos factores y contraseñas de un solo uso con contraseñas fijas es un problema puesto que estas contraseñas pueden piratearse fácilmente y puesto que son una pesadilla para que los usuarios las recuerden; y por lo tanto los usuarios eligen contraseñas fácilmente recordadas que son intrínsecamente débiles. Los usuarios también tienden a reusar las mismas contraseñas a través de múltiples aplicaciones, por lo tanto si se piratea la seguridad para una aplicación; la seguridad también puede comprometerse en muchos otros lugares.

Es un problema gestionar el acceso de usuario; es necesario que tenga lugar en una localización y bajo políticas de gobernabilidad corporativas. Es un problema que los usuarios puedan tener acceso a secretos corporativos en múltiples aplicaciones en la nube simplemente porque alguien haya olvidado eliminar sus cuentas de usuario de estos sistemas.

Es por lo tanto un problema conseguir una experiencia de Inicio de sesión sencillo para web, amigable para el usuario para usuarios de modo que una vez iniciado sesión puedan moverse entre múltiples aplicaciones de web a través de la misma sesión de explorador sin tener que iniciar sesión una y otra vez.

Es un problema también compartir servicios con socios y proveedores y establecer federación de identidad con un ajuste de configuración sencillo que permita a usuarios autenticados acceder de manera ininterrumpida a aplicaciones de los socios y que los socios puedan acceder a las suyas.

Es un problema aprovechar el verdadero potencial de un dispositivo móvil en el campo. Un proveedor de servicios desea que sus usuarios puedan autenticar y firmar transacciones en sus dispositivos móviles de una manera segura. Requieren autenticación de canal separado y firma de transacción para evitar amenazas como ataques de hombre en el explorador (MIB), de hombre en el medio (MIM) y de suplantación de identidad.

Para hacer esto necesitarán un sistema que pueda aprovisionar a los dispositivos móviles con claves secretas para autenticación y firma. Necesitarán establecer una sesión de SSL encriptada con el dispositivo, recuperar información única acerca del punto de extremo para evitar la amenaza de la clonación del dispositivo y desearán asegurar que la verificación del PIN, generación de clave, indicación de tiempo de firma y otras acciones se hagan en el lado del servidor, reduciendo de esta manera la dependencia sobre el entorno de seguridad del mismo dispositivo móvil.

Es también un problema crear un flujo de trabajo más eficaz que envíe transacciones predecibles de los dispositivos móviles de los usuarios para firma, en lugar de depender de que los usuarios inicien sesión de manera activa en una aplicación para realizar estas actividades.

El enfoque tradicional limitado a gestión de identidad simplemente no es suficiente en el mundo interconectado de hoy en día. Es un problema que las contraseñas fijas ya no sean suficiente seguras para proteger bienes e información valiosa. Las organizaciones tanto en el sector corporativo como público necesitan una solución de autenticación segura que permita un número ilimitado de usuarios, aplicaciones y dispositivos a un coste fijo. La solución también tiene que ser no intrusiva de modo que pueda integrarse con integraciones complejas con sistemas existentes.

Una y otra vez el espacio de identificación y transacción en línea relacionado con los individuos que acceden a servicios financieros y otros, el crecimiento exponencial de los dispositivos conectados en red presenta otra área de problema. La identidad de tales dispositivos conectados así como la integridad de las aplicaciones que los ejecutan, y la capacidad de estos dispositivos para cometer transacciones en su propio nombre o en nombre de un individuo u organización presenta un problema similar al anteriormente descrito - los sistemas actuales típicamente se basan en algún tipo de contraseña almacenada en tales dispositivos y usada de manera repetitiva para autenticar el dispositivo o confirmar transacciones con un proveedor de servicios.

Los sistemas en los que, por ejemplo, un “frigorífico inteligente” necesita comunicar con un servicio de reabastecimiento automatizado, un “vehículo inteligente” necesita comunicar con un servicio de vigilancia o de reparación, una cámara de velocidad necesita comunicar con un sistema de monitorización de tráfico, todos tienen el requisito de identificar de manera segura el dispositivo así como para que dicho dispositivo pueda cometer transacciones con un proveedor de servicios conectado en red.

Similar a los teléfonos móviles anteriormente mencionados, es un problema aprovisionar tales dispositivos con claves secretas para autenticación, es decir asegurar la identidad de un dispositivo cuando se conecta a un servicio en línea, y firmar, es decir cometer de manera segura transacciones con un proveedor de servicios en línea, particularmente a la luz del enrome número de tales dispositivos. Excluyendo las plataformas informáticas, un hogar típico de hoy en día puede tener una variedad de dispositivos que requieren acceso en línea - sin embargo el número de dispositivos que estarán más o menos permanentemente conectados a una red está creciendo a diario, requiere un método que sea mucho más sencillo y mucho más seguro que almacenar una contraseña estática en el dispositivo.

Solución

Con el fin de resolver uno o más de los problemas anteriormente mencionados, y desde el punto de vista de un método para establecer un secreto compartido entre un primer y un segundo dispositivo sin ninguna confianza compartida entre el primer y segundo dispositivo, para el uso de servicios proporcionados por un proveedor de servicios a un usuario del segundo dispositivo, la presente invención enseña un método donde:

a) un usuario del segundo dispositivo se identifica por el proveedor de servicios,
b) el segundo dispositivo solicita y recibe un código de activación desde el primer dispositivo,
c) el usuario del segundo dispositivo envía el código de activación al proveedor de servicios,
d) el proveedor de servicios envía el código de activación al primer dispositivo,
e) el primer dispositivo confirma el código de activación y genera y almacena el secreto compartido,
f) el primer dispositivo genera una referencia para el secreto compartido y transfiriere la referencia y el secreto

compartido al segundo dispositivo,
g) el primer dispositivo transfiriere la referencia al proveedor de servicios, y
h) el proveedor de servicios almacena la referencia y asocia la referencia al usuario.

Se propone que el usuario se identifique por el proveedor de servicios a través de una relación previamente establecida, que, como un ejemplo, puede ser a través de un método fuera de banda, tal como una visita personal o un correo certificado.

La información generada aleatoriamente única o específica de hardware puede incluirse en la solicitud del código de activación, información que puede usarse para proteger la transferencia del secreto compartido.

Se propone que la solicitud incluya información seleccionada por el usuario conocida por el usuario, tal como un código PIN, donde la información seleccionada por el usuario está disponible para detectar uso no autorizado del secreto compartido.

Para el fin de evitar uso no autorizado del segundo dispositivo debido a pérdida, robo, etc., se propone que la información seleccionada por el usuario se almacene en el primer dispositivo, no estando disponible por lo tanto localmente en el segundo dispositivo.

La presente invención enseña que el primer y segundo dispositivo validan mutuamente el secreto compartido antes de la transferencia de la referencia al proveedor de servicios.

Se propone que el segundo dispositivo inicie una interrogación periódica del primer dispositivo para el secreto compartido siguiendo la etapa b), interrogación que se termina en la finalización de la etapa f).

Se propone también que el proveedor de servicios inicie una interrogación periódica del primer dispositivo para la referencia siguiendo la etapa d), interrogación que se termina en la finalización de la etapa g).

Con el fin de proporcionar escalabilidad la presente invención enseña que el primer dispositivo puede establecer un secreto compartido con más de un segundo dispositivo, que el segundo dispositivo puede establecer un secreto compartido con más de un primer dispositivo, y que el primer dispositivo puede proporcionar el uso de secretos compartidos establecidos a más de un proveedor de servicios.

Debería entenderse que el primer dispositivo y el proveedor de servicios pueden ser dos unidades físicas separadas o dos unidades lógicas separadas en una y la misma unidad física.

La presente invención también se refiere a un sistema adaptado para establecer un secreto compartido entre un primer y un segundo dispositivo sin ninguna confianza compartida entre dicho primer y segundo dispositivo, para el uso de servicios proporcionados por un proveedor de servicios a un usuario del segundo dispositivo. La presente invención enseña específicamente que,

a) el segundo dispositivo está adaptado para posibilitar que un usuario se identifique por el proveedor de servicios,
b) el segundo dispositivo está adaptado para solicitar y recibir un código de activación desde el primer dispositivo,
c) el proveedor de servicios está adaptado para recibir el código de activación desde el usuario del segundo dispositivo,
d) el proveedor de servicios está adaptado para enviar el código de activación al primer dispositivo,
e) el primer dispositivo está adaptado para confirmar el código de activación y generar y almacenar el secreto compartido,
f) el primer dispositivo está adaptado para generar una referencia para el secreto compartido y para transferir la referencia y el secreto compartido al segundo dispositivo,
g) el primer dispositivo está adaptado para transferir la referencia al proveedor de servicios, y
h) el proveedor de servicios está adaptado para almacenar la referencia y para asociar la referencia al usuario.

El proveedor de servicios puede estar adaptado para identificar el usuario a través de una relación previamente establecida o a través de un método fuera de banda, tal como una visita personal o un correo certificado.

El segundo dispositivo puede estar adaptado para incluir información generada aleatoriamente o específica de hardware único en la solicitud del código de activación, y el primer dispositivo puede estar adaptado para usar esta información para proteger la transferencia del secreto compartido.

Se propone que el segundo dispositivo esté adaptado para incluir información seleccionada por el usuario conocida por el usuario en la solicitud, donde la información seleccionada por el usuario está disponible para el primer dispositivo para detectar uso no autorizado del secreto compartido.

Para evitar el uso no autorizado del segundo dispositivo, tal como en el caso de pérdida, robo, etc., se propone que el primer dispositivo esté adaptado para almacenar la información seleccionada por el usuario de modo que la información seleccionada por el usuario no esté disponible localmente en el segundo dispositivo.

La presente invención enseña que el primer y segundo dispositivo pueden estar adaptados para validar mutuamente el secreto compartido antes de la transferencia de la referencia al proveedor de servicios.

Se propone que siguiendo la etapa b) el segundo dispositivo está adaptado para iniciar una interrogación periódica del primer dispositivo para el secreto compartido, interrogación que se termina en la finalización de la etapa f).

Se propone también que siguiendo la etapa d) el proveedor de servicios está adaptado para iniciar una interrogación periódica del primer dispositivo para la referencia, interrogación que se termina en la finalización de la etapa g).

Para posibilitar escalabilidad se propone que el primer dispositivo esté adaptado para establecer un secreto compartido con más de un segundo dispositivo, que el segundo dispositivo esté adaptado para establecer un secreto compartido con más de un primer dispositivo, y que el primer dispositivo esté adaptado para proporcionar el uso de secretos compartidos establecidos a más de un proveedor de servicios.

El primer dispositivo y el proveedor de servicios pueden ser dos unidades físicas separadas o dos unidades lógicas separadas en una y la misma unidad física.

La presente invención también se refiere a un producto de programa informático que comprende código de programa informático, que, cuando se ejecuta mediante un dispositivo, posibilita que el dispositivo realice las etapas de un primer dispositivo de acuerdo con el método inventivo.

La presente invención también se refiere a un producto de programa informático que comprende código de programa informático, que, cuando se ejecuta mediante un dispositivo, posibilita que el dispositivo realice las etapas de un segundo dispositivo de acuerdo con el método inventivo.

La presente invención también se refiere a un producto de programa informático que comprende código de programa informático, que, cuando se ejecuta mediante un dispositivo, posibilita que el dispositivo realice las etapas de un proveedor de servicios de acuerdo con el método inventivo.

La presente invención también se refiere a un medio legible por ordenador que lleva código de programa informático de acuerdo con uno cualquiera de los productos de programa informático inventivos.

Ventajas

Las ventajas de la presente invención es que proporciona una familia de productos en las áreas de autenticación de usuarios, aprovisionamiento de credenciales IDP (Proveedor de Identidad) en la nube, SSO de Web y firma de transacción móvil, y estos productos pueden implementarse fácilmente como una aplicación de autenticación y firma de transacción para diferentes dispositivos tales como dispositivos iOS y Android.

Excepto para las aplicaciones móviles la invención puede implementarse como aparatos físicos o virtuales integrados en una plataforma de desarrollo común, por ejemplo, con un sistema operativo basado en Linux consolidado. La invención proporciona productos que son fáciles de usar, desarrollar y mantener, que superan a la competencia y proporcionan tecnología de la siguiente generación a precio muy competitivo.

Aunque el aparato de autenticación típicamente reside detrás de un cortafuegos, los otros aparatos están orientados a la nube. Para facilidad de desarrollo y reducir el ciclo de ventas estos aparatos pueden desplegarse en un servidor “multi-versión”, que significa que el aparato relevante puede conectarse con conmutadores de licencia como y cuando el cliente los requiera.

En un flujo de trabajo que requiere múltiples autorizaciones, por ejemplo gran valor de transacción en tesorería y banca comercial, la presente invención podría usarse para enviar solicitudes de autorización secuencialmente a los diferentes dispositivos móviles de los gestores, reduciendo drásticamente el tiempo de transacción y tara administrativa.

La presente invención proporciona un acceso seguro de gestión de servidor de autenticación fuerte de la siguiente generación para redes corporativas. Está basado en un modelo único de precios donde los costes son independientes del número de usuarios, que posibilita que los clientes tomen un enfoque ilimitado que incluye todos los empleados, socios y clientes en el sistema, conectándolos a cualquier aplicación usando una amplia gama de dispositivos.

Breve descripción de los dibujos

Un método, dispositivo y producto de programa informático de acuerdo con la presente invención se describirán ahora en detalle con referencia a los dibujos adjuntos, en los que:

La Figura 1 es la ilustración esquemática y simplificada que muestra el aprovisionamiento de un secreto compartido,
La Figura 2 es un diagrama de secuencia que explica el protocolo realizado por las interacciones entre una aplicación de testigo móvil, un servidor de aprovisionamiento y una aplicación de banca en línea,
La Figura 3 es un diagrama de estado que muestra los estados a través de los que pasa un servidor de aprovisionamiento cuando maneja un aprovisionamiento de testigo,
La Figura 4 es un diagrama de estado que muestra los estados a través de los que pasa un testigo móvil cuando maneja un aprovisionamiento de testigo,
La Figura 5 es una ilustración esquemática y simplificada del uso de un secreto compartido en un proceso de transacción, y
La Figura 6 es un diagrama de secuencia que explica el protocolo realizado por las interacciones entre la aplicación de testigo móvil 2', el servidor de aplicación móvil 1' y la aplicación de banca en línea 3

Descripción de las realizaciones actualmente preferidas

La presente invención se describirá ahora con referencia a la figura 1 que muestra el aprovisionamiento de un secreto compartido, que en la descripción se denominará un testigo móvil. La sección 'casos de uso' trata sobre el procedimiento desde un punto de vista del usuario final, mientras que la 'vista general de sistema' proporciona una descripción técnica en profundidad.

En las siguientes realizaciones ejemplares el primer dispositivo 1 se ejemplifica mediante un servidor de aprovisionamiento 1 y un servidor de transacción 1', y el segundo dispositivo 2 se ejemplifica mediante un dispositivo móvil 2 con una aplicación de testigo móvil 2'. El proveedor de servicios 3 se ejemplifica mediante una aplicación de banca en línea 3, que puede accederse por medio de un ordenador personal 2". Un usuario 4 puede acceder a la aplicación de banca en línea 3 a través del ordenador personal 2" y a la aplicación de testigo móvil 2' a través del dispositivo móvil 2. Debería entenderse que el ordenador personal 2" puede ser cualquier tipo de dispositivo informático disponible para el usuario 4 y que el dispositivo móvil 2 puede ser cualquier tipo de dispositivo móvil disponible para el usuario 4. Debería entenderse también que el ordenador personal 2" y el dispositivo móvil 2 pueden ser uno y el mismo dispositivo donde la aplicación de banca en línea 3 y la aplicación de testigo móvil 2' puede accederse y ejecutarse simultáneamente como dos aplicaciones separadas.

Casos de uso

La Figura 1 ilustra un escenario en el que se supone que el testigo o secreto compartido se ha de usar para banca en línea; el aprovisionamiento para clientes distintos de los bancos tendría una forma algo diferente.

Son posibles dos casos: un usuario existente, que ya tiene credenciales registrados con el banco, desea empezar a usar un testigo móvil, y un nuevo usuario está configurando una cuenta bancaria y desea obtener un testigo móvil.

El primer caso es el más sencillo de los dos, puesto que trata con un usuario existente 4 que ya tiene credenciales con el banco 3' y los usa para acceder a la aplicación de banca en línea 3 para realizar pagos en línea y similares. La misma aplicación se usa durante aprovisionamiento de testigo móvil.

Las etapas que el usuario toma son como sigue:

- El usuario 4 inicia sesión en la aplicación de banca en línea 3 con un nombre de usuario y contraseña estática.
- Siguiendo las instrucciones en la aplicación de banca en línea, el usuario 4 instala la aplicación de testigo 2' en su teléfono móvil 2.
- Se genera un código de activación, se envía a la aplicación móvil 2' y se presenta en la pantalla, se lee o se hace conocer para el usuario 4 de alguna otra manera adecuada por medio del teléfono móvil 2.
- El usuario 4 escribe el código de activación en una página apropiada en la aplicación de banca en línea 3.
- En este punto, el usuario 4 configura el PIN que de ahora en adelante se usará para acceder a la aplicación de testigo 2'.
- Se aprovisiona el testigo y el usuario observa un mensaje de confirmación tanto en la aplicación de banca en línea 3 como en la aplicación de testigo 2'.

El segundo caso se refiere a un nuevo usuario 4, que desea obtener un testigo móvil al mismo tiempo que abre una cuenta bancaria.

Las etapas que el usuario toma son como sigue:

- El usuario 4 recibe un código de activación de un solo uso para acceder a la aplicación de banca en línea 3. Este código es únicamente usable para aprovisionamiento de testigo móvil, no para el uso normal de la aplicación.

  a) El código de activación puede recibirse a través de varios canales, de acuerdo con la elección del banco 3' y/o el usuario final 4:
  b) entregarse a la dirección local del usuario por correo. En este caso el código es válido durante un periodo de tiempo más largo, tal como cinco o diez días.
  c) Si el número de teléfono móvil del usuario está registrado con el banco, el código puede entregarse por SMS. En este caso el código es válido durante un periodo de tiempo más corto, por ejemplo unos pocos minutos.
  d) Si la dirección de correo electrónico del usuario está registrada con el banco, el código puede entregarse mediante correo electrónico. De manera similar a SMS, en este caso el código es válido para un periodo de tiempo más corto.

- El usuario 4 accede a la aplicación de banca en línea 3 y sigue las instrucciones para descargar la aplicación de testigo 2'. El resto del procedimiento es el mismo que para usuarios del banco existentes.

La arquitectura de sistema e interacciones entre componentes del sistema se describirán ahora en más detalle.

Inicialmente se describirá el aprovisionamiento de testigo.

El usuario 4 navega 11 a una aplicación de banca en línea 3. En este punto se le instruye cómo instalar e iniciar una aplicación de testigo móvil 2'. Se le instruye también leer un código de activación desde la aplicación de testigo móvil 2' y escribirlo en la aplicación de banca en línea 3 para confirmación.

Después de que el usuario enciende la aplicación de testigo móvil 2', solicita 12 un código de activación desde un servidor de aprovisionamiento 1.

a. la aplicación de testigo móvil 2' envía una solicitud para un código de activación, que incluye identificadores generados aleatoriamente o, si están disponibles, específicos de hardware, tales como IMEI, número de teléfono etc.
b. el servidor de aprovisionamiento 1 genera un código de activación, lo almacena junto con la información específica de hardware y devuelve el código de activación a la aplicación de testigo móvil.

i. El código de activación reside en el servidor de aprovisionamiento 1 hasta la finalización del proceso de aprovisionamiento. Si el aprovisionamiento de testigo no se ha completado dentro de un intervalo de tiempo establecido, tal como 5 minutos, el código de activación se borra automáticamente.

c. la aplicación de testigo móvil 2' hace el código de activación disponible para el usuario 4, por ejemplo presentándolo para que el usuario 4 lo lea.
d. la aplicación de testigo móvil 2' también empieza a interrogar el servidor de aprovisionamiento 1 para una semilla de testigo. El servidor de aprovisionamiento 1 responde con un mensaje de 'semilla no disponible' hasta que se verifica el código de activación a través de la aplicación de banca en línea 3.

El usuario 4 introduce 13 el código de activación en la aplicación de banca en línea 3.

La aplicación de banca en línea 3 envía 14 el código de activación al servidor de aprovisionamiento 1.

a. El servidor de aprovisionamiento 1 verifica el código de activación
b. La aplicación de banca en línea 3 empieza a interrogar al servidor de aprovisionamiento 1 para información sobre si el testigo está personalizado. El servidor de aprovisionamiento 1 responde con 'testigo no personalizado'.

El servidor de aprovisionamiento 1 genera 15 una semilla de testigo por sí mismo, o por medio de un módulo de seguridad de hardware 5 donde los requisitos de regulación, de política de seguridad o de auditoría así lo postulan, para asegurar buena aleatoriedad de la semilla de testigo.

a. La semilla de testigo puede encriptarse de dos maneras diferentes, generando de esta manera dos encriptaciones de semilla.

i. Se encripta una semilla de testigo usando una clave de transporte derivada de la información específica de hardware y un secreto compartido entre la aplicación de testigo móvil 2' y el servidor de aprovisionamiento 1.

La semilla_{HSI} de testigo se usará para enviar de manera segura la semilla de testigo a la aplicación de testigo móvil 2'.

ii. Una semilla de testigo puede encriptarse también con una clave de transporte desde un componente de validación OATH/OCRA 6.

La $semilla_{OATH/OCRA}$ de testigo se usará para enviar de manera segura la semilla de testigo al componente de validación de OATH/OCRA.

b. Se obtiene un número de serie de testigo desde el componente de validación de OATH/OCRA.
c. Tanto la $semilla_{HSI}$ de testigo como la $semilla_{ATH/OCRA}$ de testigo juntas con el número de serie de testigo se graban en el servidor de aprovisionamiento 1.

La $semilla_{HSI}$ se envía 16 a la aplicación de testigo móvil 2' junto con el número de serie de testigo; la aplicación de testigo móvil 2' estaba interrogando la semilla de testigo todo el tiempo.

La aplicación de testigo móvil 2' envía 17 una solicitud para verificación de una contraseña de un solo uso al servidor de aprovisionamiento 1.

a. Después de recibir la semilla de testigo, la aplicación de testigo móvil 2' la desencripta.
b. la aplicación de testigo móvil 2' genera una contraseña de un solo uso
c. la aplicación de testigo móvil 2' envía la contraseña de un solo uso y el número de serie de testigo al servidor de aprovisionamiento 1 para verificación.

El servidor de aprovisionamiento 1 recibe la solicitud de verificación de contraseña de un solo uso.

a. El servidor de aprovisionamiento 1 envía 18 la solicitud de verificación (OTP+ número de serie de testigo+ $semilla_{OATH/OCRA}$ de testigo+detalles de testigo) a un componente de validación OATH/OCRA 6.
b. El componente de validación de OATH/OCRA 6' señaliza su aprobación al servidor de aprovisionamiento 1, y la respuesta se reenvía a la aplicación de testigo móvil 2'.
c. La aplicación de testigo móvil 2' ahora está personalizada satisfactoriamente.

La interrogación de la aplicación de banca en línea 3 se responde ahora 19 con un mensaje de aprovisionamiento de testigo satisfactorio que contiene el número de serie de testigo. Se notifica al usuario de que el proceso de aprovisionamiento está finalizado.

La aplicación de banca en línea 3 asocia 110 el usuario 4 con el número de serie de testigo en el repositorio del usuario del banco 7.

Es posible requerir que el usuario 4 establezca un secreto compartido entre el servidor de aprovisionamiento 1 y la aplicación de testigo móvil 2' en el comienzo del proceso de aprovisionamiento, por ejemplo con uso de código de QR o código introducido por el usuario. Este secreto compartido se usaría para proteger los datos intercambiados entre las dos partes. También, más tarde, durante los procesos de transacción este secreto podría usarse también para las mismas razones como se han mencionado anteriormente. Este secreto se mantendría en la aplicación de testigo móvil 2' encriptado bajo un PIN que únicamente conoce el usuario.

La Figura 2 es un diagrama de secuencia que explica el protocolo realizado por las interacciones entre la aplicación de testigo móvil MT 2', el servidor de aprovisionamiento PS 1 y aplicación de banca en línea BOA 3.

La Figura 3 es un diagrama de estado que muestra los estados a través de los que pasa el servidor de aprovisionamiento cuando maneja un aprovisionamiento de testigo.

La Figura 4 es un diagrama de estado que muestra los estados a través de los que pasa el testigo móvil cuando maneja un aprovisionamiento de testigo.

El proceso de una validación de transacción se describirá ahora. Este proceso puede referirse a que el usuario 4 esté intentando iniciar sesión en una aplicación de banca en línea 3 o para validar una transacción que se está realizando a través de la misma aplicación. Las etapas que el usuario toma son como sigue:

- El usuario explora la aplicación de banca en línea 3 e introduce sus credenciales de usuario o solicita que se realice una transacción.
- La aplicación de banca en línea 3 instruye al usuario 4 a que inicie la aplicación de testigo móvil 2' en su teléfono 2.
- La aplicación de testigo móvil 2' recibe información con respecto a la transacción en cuestión y se requiere que el usuario 4 confirme la acción.

La Figura 5 muestra la arquitectura de sistema e interacciones entre componentes del sistema, donde se ilustra el proceso de transacción con todos los detalles relevantes.

El usuario 4 intenta iniciar sesión 51 en la aplicación de banca en línea 3 o si ya ha iniciado sesión intenta realizar una transacción.

La aplicación de banca en línea 3 obtiene el nombre de usuario del usuario y lo mapea 52 a un número de serie en un repositorio de cuentas de usuario local 7.

La aplicación de banca en línea 3 envía 53 un mensaje al servidor de aplicación móvil 1', mensaje que contiene:

a. Número de serie del usuario
b. Texto de transacción - (por ejemplo "Transferir 1000 euros a número de cuenta xxxxxxxxxxxx")

El servidor de aplicación móvil 1' responde 54 con una referencia de transacción (TRREF) que es una referencia generada aleatoriamente única para la transacción. Esta referencia identifica inequívocamente cada transacción y sirve como un id de sesión.

a. Después de esta etapa la aplicación de banca en línea 3 pide continuamente al servidor de aplicación móvil 1' el estado de la transacción con una referencia de transacción TRREF.
b. el servidor de aplicación móvil 1' informa a la aplicación de banca en línea 3 sobre cualquier cambio del estado.

La aplicación de banca en línea 3 pide 55 al usuario que inicie su aplicación de testigo móvil 2'.

La aplicación de testigo móvil 2' cuando se enciende pide al usuario que introduzca el PIN que el usuario elige durante el aprovisionamiento de la aplicación de testigo móvil 2'. Este PIN se usa para proteger datos confidenciales mantenidos en el dispositivo móvil. De esta manera no hay datos sensibles en texto sin cifrar presentes en la memoria o almacenamiento del dispositivo.

a. La verificación de PIN no se realiza en la aplicación de testigo móvil 2', sino en el servidor de aplicación móvil 1'. Cuando se introduce el PIN, se usa para desencriptar los datos sensibles.
b. Estos datos, incluso aunque pudieran estar incorrectos, se usan en el resto de la verificación de la transacción.
c. Esto conducirá a fallo de verificación de transacción y un usuario tendría que repetir el proceso.
d. Si el PIN se introduce de manera errónea demasiadas veces la aplicación de testigo móvil 2' puede borrar todos los datos y el usuario 4 debería pasar a través del proceso de aprovisionamiento de nuevo. El servidor de aplicación móvil 1' también puede bloquear que una instancia de este tipo de la aplicación de testigo móvil 2' funcione de nuevo hasta que se vuelva a aprovisionar que, a su vez, requiere probar la identidad del usuario 4 de nuevo.
e. Después de que se introduce el PIN correcto la aplicación de testigo móvil 2' pide 56 al servidor de aplicación móvil 1' si hay transacciones pendientes. Este mensaje contiene el número de serie del usuario, un desafío nuevamente generado y respuesta apropiada. Esta respuesta se introduce para mitigar la posibilidad de que un atacante lea los datos de la transacción.

El servidor de aplicación móvil 1' verifica 57 el par desafío-respuesta con el componente de validación de OATH/OCRA 6. Si la verificación es satisfactoria a continuación se envía 58 la referencia de transacción TRREF y el texto de transacción a la aplicación de testigo móvil 2'.

La aplicación de testigo móvil 2' calcula una RESPUESTA y la envía 59 junto con la referencia de transacción recibida TRREF.

El servidor de aplicación móvil 1' verifica 510 el par desafío-respuesta con el componente de validación de OATH/OCRA 6.

Si el componente de validación de OATH/OCRA 6 verifica la respuesta el servidor de aplicación móvil 1' notifica 511, 512 a la aplicación de testigo móvil 2' y a la aplicación de banca en línea 3 que la transacción fue satisfactoria.

Se propone que la comunicación entre el servidor de aplicación móvil 1' y la aplicación de banca en línea 3 y la aplicación de testigo móvil 2' se proteja por el uso del protocolo de TLS.

Se propone también que si durante el proceso de aprovisionamiento se estableció un secreto compartido entre el servidor de aprovisionamiento 1 y la aplicación de testigo móvil 2', entonces este podría usarse para proteger datos intercambiados entre estas partes.

La Figura 6 es un diagrama de secuencia que explica el protocolo realizado por las interacciones entre la aplicación de testigo móvil MT 2', el servidor de aplicación móvil MAS 1' y la aplicación de banca en línea BOA 3.

En las realizaciones ejemplares el uso de un servidor de aprovisionamiento, servidor de aplicación móvil, un componente de validación OATH/OCRA y un módulo de seguridad de hardware se han mostrado como

componentes separados, sin embargo, debería entenderse que tanto el servidor de aprovisionamiento 1 como el servidor de aplicación móvil 1' pueden incluir la función de uno o ambos del componente de validación de OATH/OCRA 6 y el módulo de seguridad de hardware 5 y que uno y el mismo servidor puede funcionar tanto como un servidor de aprovisionamiento 1 como un servidor de aplicación móvil 1'. En las reivindicaciones el primer dispositivo se describe como que comprende todas estas funciones. El experto en la materia entiende que el primer dispositivo puede realizarse a través de uno o varios servidores a través de los que estos servidores y funciones se hacen disponibles tanto a través de funciones internas como servicios externos.

En las realizaciones ejemplares se ha usado un banco en línea para ejemplificar un proveedor de servicios, sin embargo, debería entenderse que la expresión "proveedor de servicio" incluye cualquier tipo de proveedor donde se requiera el acceso protegido al servicio, tal como aplicaciones de web o en la nube donde se requiere una identificación segura de un usuario, cualquier tipo de transacción económica, y acceso a material protegido y redes corporativas.

Se entenderá que la invención no está restringida a las realizaciones ejemplares anteriormente descritas e ilustradas de las mismas y que pueden realizarse modificaciones dentro del alcance de la invención como se define mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para establecer un secreto compartido entre un primer y un segundo dispositivo (1, 2) sin ninguna confianza compartida entre dicho primer y segundo dispositivo, para el uso de servicios proporcionados por un proveedor de servicios (3') a un usuario (4) de dicho segundo dispositivo (2), caracterizado por que,

a) dicho usuario (4) de dicho segundo dispositivo (2) está identificado (11) por dicho proveedor de servicios (3),
b) dicho segundo dispositivo (2) solicita (12) y recibe un código de activación desde dicho primer dispositivo (1),
c) dicho usuario (4) de dicho segundo dispositivo envía (13) dicho código de activación a dicho proveedor de servicios (3),
d) dicho proveedor de servicios (3) envía (14) dicho código de activación a dicho primer dispositivo (1),
e) dicho primer dispositivo (1) confirma dicho código de activación y genera y almacena dicho secreto compartido (15),
f) dicho primer dispositivo (1) genera una referencia para dicho secreto compartido y transfiere (16) dicha referencia y secreto compartido a dicho segundo dispositivo (2),
g) dicho primer dispositivo (1) transfiere (19) dicha referencia a dicho proveedor de servicios (3), y
h) dicho proveedor de servicios (3) almacena (110) dicha referencia y asocia dicha referencia a dicho usuario (4).

2. Un método de acuerdo con la reivindicación 1, caracterizado por que dicho usuario se identifica por dicho proveedor de servicios a través de una relación previamente establecida.

3. Un método de acuerdo con la reivindicación 1, caracterizado por que dicho usuario se identifica por dicho proveedor de servicios a través de un método fuera de banda, tal como una visita personal o un correo certificado.

4. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que se incluye información única generada aleatoriamente o específica de hardware en dicha solicitud de código de activación, y por que dicha información se usa para proteger la transferencia de dicho secreto compartido.

5. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que dicha solicitud incluye información seleccionada por el usuario conocida por dicho usuario, estando disponible dicha información seleccionada por el usuario para detectar el uso no autorizado de dicho secreto compartido.

6. Un método de acuerdo con la reivindicación 5, caracterizado por que dicha información seleccionada por el usuario se almacena en dicho primer dispositivo.

7. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que, antes de la transferencia de dicha referencia a dicho proveedor de servicios, dicho primer y segundo dispositivo validan mutuamente dicho secreto compartido.

8. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por, siguiendo la etapa b), dicho segundo dispositivo inicia una interrogación periódica de dicho primer dispositivo para dicho secreto compartido, y termina dicha interrogación en la finalización de la etapa f).

9. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que, siguiendo la etapa d), dicho proveedor de servicios inicia una interrogación periódica de dicho primer dispositivo para dicha referencia, y termina dicha interrogación en la finalización de la etapa g).

10. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que dicho primer dispositivo puede establecer un secreto compartido con más de un segundo dispositivo.

11. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que dicho segundo dispositivo puede establecer un secreto compartido con más de un primer dispositivo.

12. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que dicho primer dispositivo puede proporcionar el uso de secretos compartidos establecidos a más de un proveedor de servicios.

13. Un método de acuerdo con cualquier reivindicación anterior, caracterizado por que dicho primer dispositivo y dicho proveedor de servicios son dos unidades físicas separadas o dos unidades lógicas separadas en una y la misma unidad física.

14. Un sistema adaptado para establecer un secreto compartido entre un primer y un segundo dispositivo sin ninguna confianza compartida entre dicho primer y segundo dispositivo, para el uso de servicios proporcionados por un proveedor de servicios a un usuario de dicho segundo dispositivo, caracterizado por que,

a) dicho segundo dispositivo está adaptado para posibilitar que se identifique dicho usuario por dicho proveedor de servicios,

b) dicho segundo dispositivo está adaptado para solicitar y recibir un código de activación desde dicho primer dispositivo,
c) dicho proveedor de servicios está adaptado para recibir dicho código de activación desde el usuario de dicho segundo dispositivo,
d) dicho proveedor de servicios está adaptado para enviar dicho código de activación a dicho primer dispositivo,
e) dicho primer dispositivo está adaptado para confirmar dicho código de activación y generar y almacenar dicho secreto compartido,
f) dicho primer dispositivo está adaptado para generar una referencia para dicho secreto compartido y para transferir dicha referencia y secreto compartido a dicho segundo dispositivo,
g) dicho primer dispositivo está adaptado para transferir dicha referencia a dicho proveedor de servicios, y
h) dicho proveedor de servicios está adaptado para almacenar dicha referencia y para asociar dicha referencia a dicho usuario.

15. Un sistema de acuerdo con la reivindicación 14, caracterizado por que dicho proveedor de servicios está adaptado para identificar dicho usuario a través de una relación previamente establecida.

16. Un sistema de acuerdo con la reivindicación 14, caracterizado por que dicho proveedor de servicios está adaptado para identificar dicho usuario a través de un método fuera de banda, tal como una visita personal o un correo certificado.

17. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 16, caracterizado por que dicho segundo dispositivo está adaptado para incluir información única generada aleatoriamente o específica de hardware en dicha solicitud de código de activación, y por que dicho primer dispositivo está adaptado para usar dicha información para proteger la transferencia de dicho secreto compartido.

18. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 17, caracterizado por que dicho segundo dispositivo está adaptado para incluir información seleccionada por el usuario conocida por dicho usuario en dicha solicitud, estando disponible dicha información seleccionada por el usuario para dicho primer dispositivo para detectar el uso no autorizado de dicho secreto compartido.

19. Un sistema de acuerdo con la reivindicación 18, caracterizado por que dicho primer dispositivo está adaptado para almacenar dicha información seleccionada por el usuario.

20. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 19, caracterizado por que dicho primer y segundo dispositivo están adaptados para validar mutuamente dicho secreto compartido antes de la transferencia de dicha referencia a dicho proveedor de servicios.

21. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 20, caracterizado por que siguiendo la etapa b) dicho segundo dispositivo está adaptado para iniciar una interrogación periódica de dicho primer dispositivo para dicho secreto compartido, interrogación que se termina en la finalización de la etapa f).

22. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 21, caracterizado por que siguiendo la etapa d) dicho proveedor de servicios está adaptado para iniciar una interrogación periódica de dicho primer dispositivo para dicha referencia, interrogación que se termina en la finalización de la etapa g).

23. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 22, caracterizado por que dicho primer dispositivo está adaptado para establecer un secreto compartido con más de un segundo dispositivo.

24. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 23, caracterizado por que dicho segundo dispositivo está adaptado para establecer un secreto compartido con más de un primer dispositivo.

25. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 24, caracterizado por que dicho primer dispositivo está adaptado para proporcionar el uso de secretos compartidos establecidos a más de un proveedor de servicios.

26. Un sistema de acuerdo con una cualquiera de las reivindicaciones 14 a 25, caracterizado por que dicho primer dispositivo y dicho proveedor de servicios son dos unidades físicas separadas o dos unidades lógicas separadas en una y la misma unidad física.

27. Un producto de programa informático que comprende código de programa informático, que, cuando se ejecuta mediante un dispositivo, posibilita que dicho dispositivo realice las etapas de un primer dispositivo de acuerdo con una cualquiera de las reivindicaciones 1, 4, 5, 6, 7, 8, 10 o 12.

28. Un producto de programa informático que comprende código de programa informático, que, cuando se ejecuta mediante un dispositivo, posibilita que dicho dispositivo realice las etapas de un segundo dispositivo de acuerdo con una cualquiera de las reivindicaciones 1, 4, 5, 7 u 11.

29. Un producto de programa informático que comprende código de programa informático, que, cuando se ejecuta mediante un dispositivo, posibilita que dicho dispositivo realice las etapas de un proveedor de servicios de acuerdo con una cualquiera de las reivindicaciones 1, 2, 3 u 8.

30. Un medio legible por ordenador caracterizado por llevar código de programa informático de acuerdo con una cualquiera de las reivindicaciones 27 a 29.

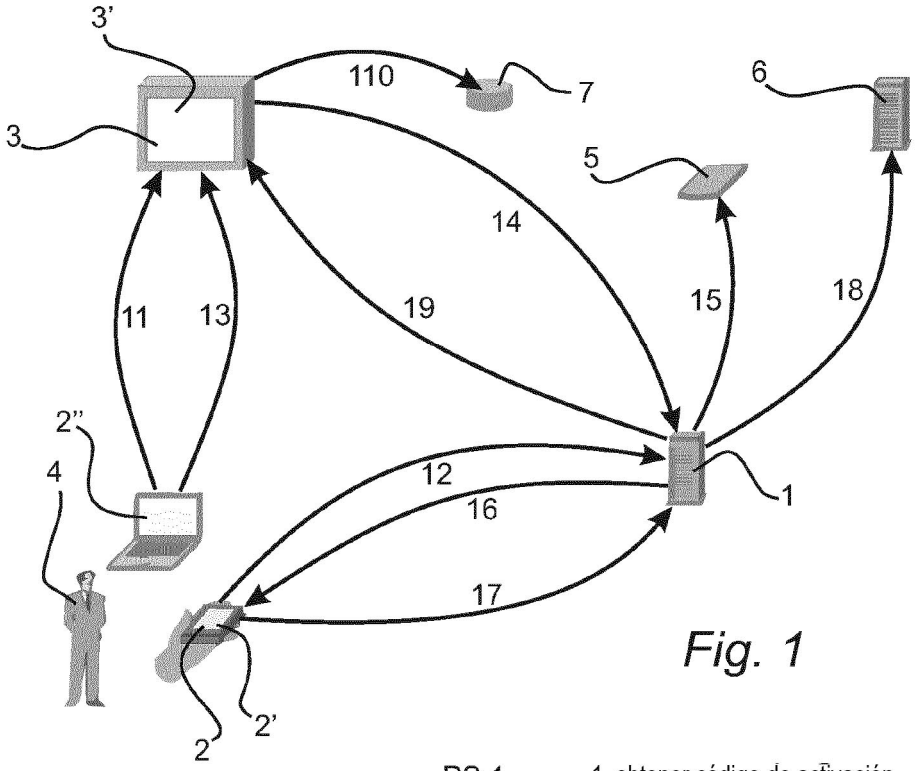
3'
110
7
6
3
5
14
11
13
19
15
18
2"
4
12
1
16
17
2'
2

Fig. 1

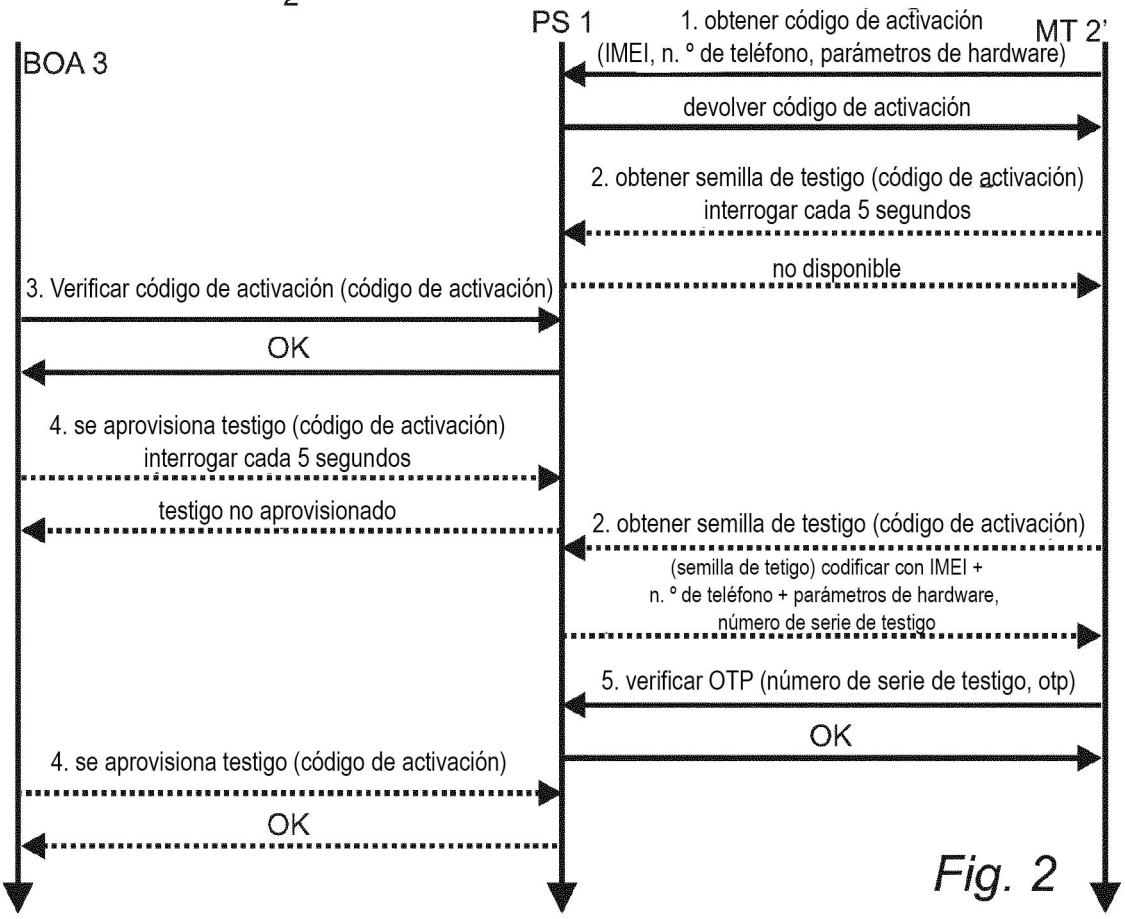
PS 1
1. obtener código de activación
(IMEI, n. º de teléfono, parámetros de hardware)
MT 2'
BOA 3
devolver código de activación
2. obtener semilla de testigo (código de activación)
interrogar cada 5 segundos
no disponible
3. Verificar código de activación (código de activación)
OK
4. se aprovisiona testigo (código de activación)
interrogar cada 5 segundos
testigo no aprovisionado
2. obtener semilla de testigo (código de activación)
(semilla de tetigo) codificar con IMEI +
n. º de teléfono + parámetros de hardware,
número de serie de testigo
5. verificar OTP (número de serie de testigo, otp)
OK
4. se aprovisiona testigo (código de activación)
OK

Fig. 2

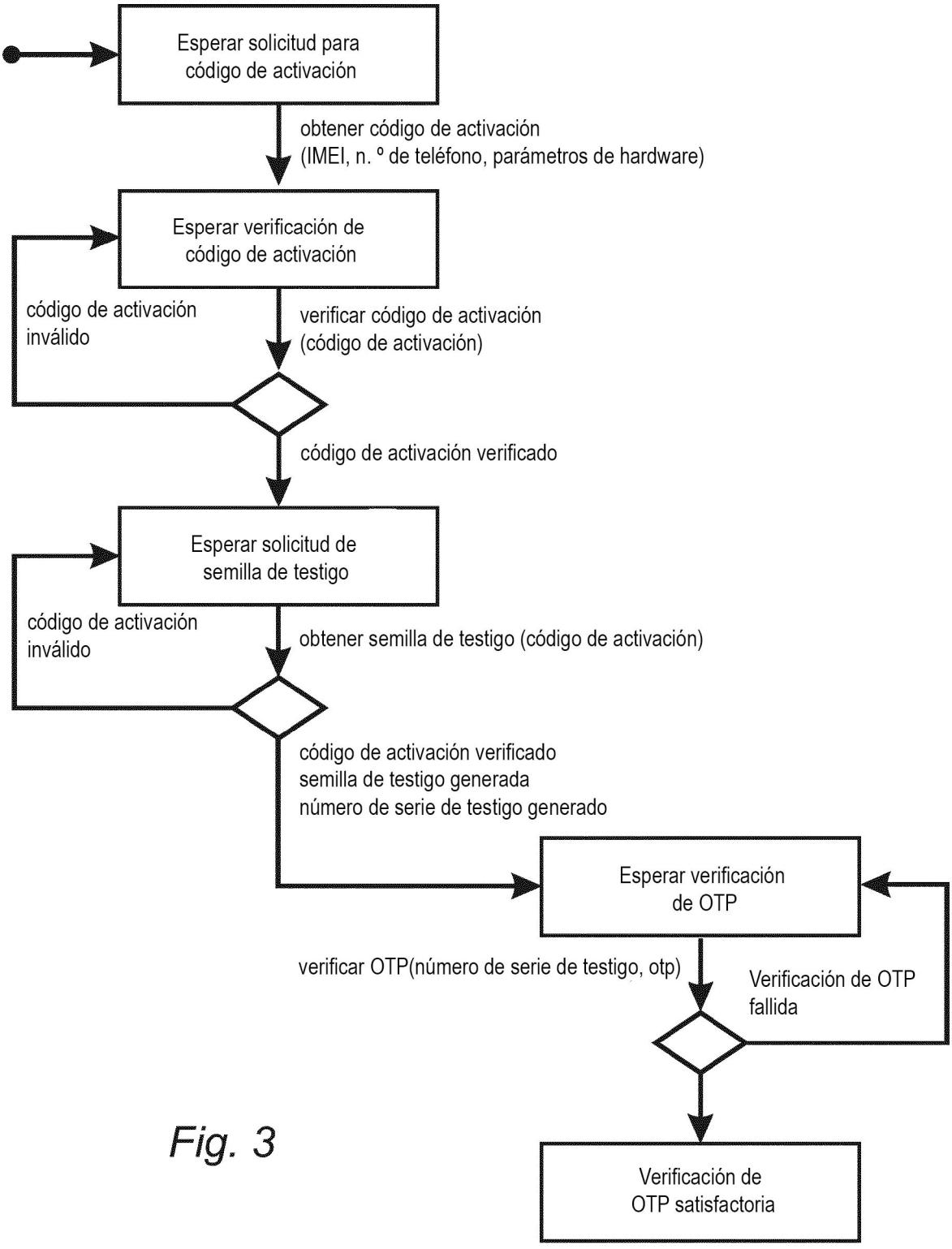
Esperar solicitud para código de activación
obtener código de activación (IMEI, n. º de teléfono, parámetros de hardware)
Esperar verificación de código de activación
código de activación inválido
verificar código de activación (código de activación)
código de activación verificado
Esperar solicitud de semilla de testigo
código de activación inválido
obtener semilla de testigo (código de activación)
código de activación verificado
semilla de testigo generada
número de serie de testigo generado
Esperar verificación de OTP
verificar OTP(número de serie de testigo, otp)
Verificación de OTP fallida
Verificación de OTP satisfactoria

Fig. 3

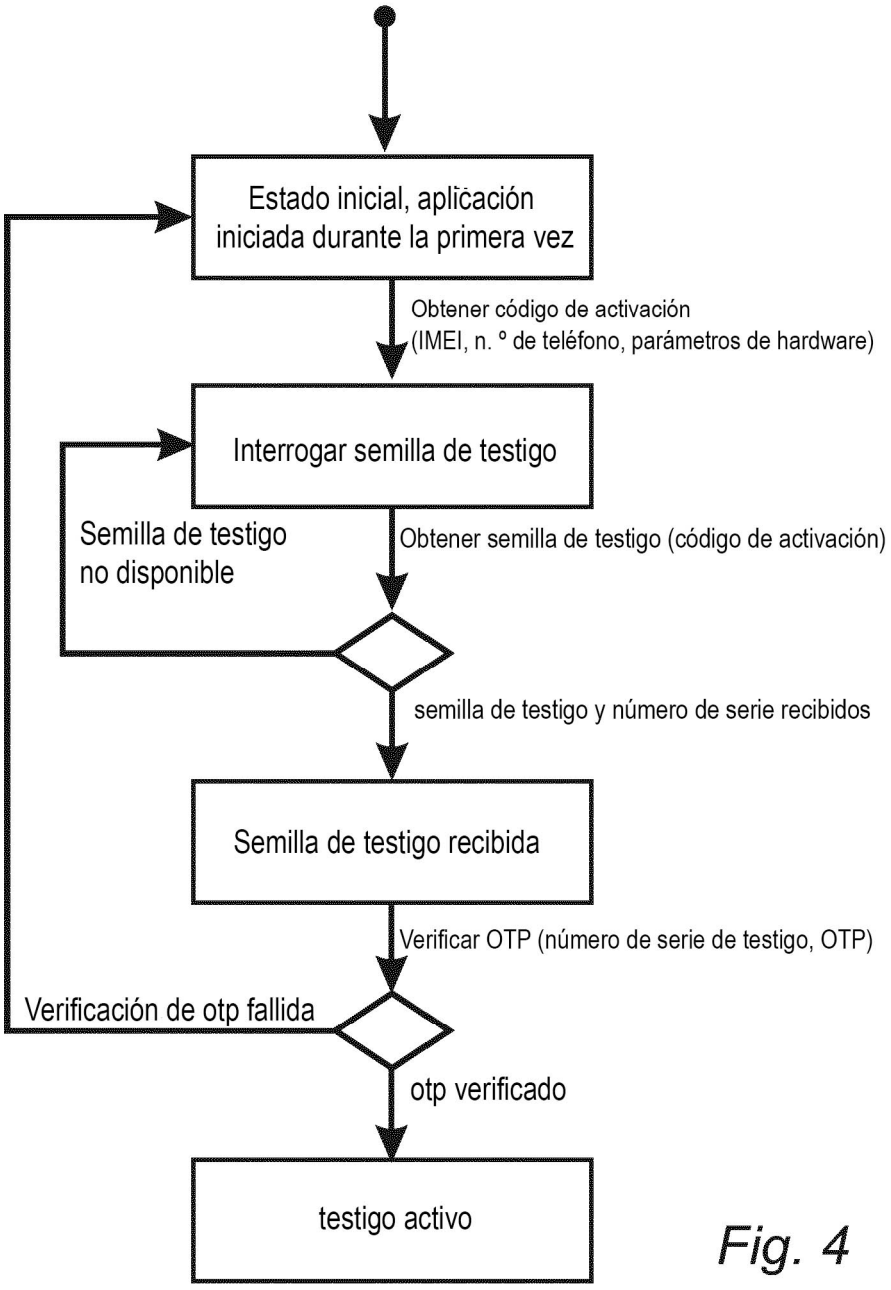
Estado inicial, aplicación iniciada durante la primera vez
Obtener código de activación (IMEI, n. º de teléfono, parámetros de hardware)
Interrogar semilla de testigo
Semilla de testigo no disponible
Obtener semilla de testigo (código de activación)
semilla de testigo y número de serie recibidos
Semilla de testigo recibida
Verificar OTP (número de serie de testigo, OTP)
Verificación de otp fallida
otp verificado
testigo activo

Fig. 4

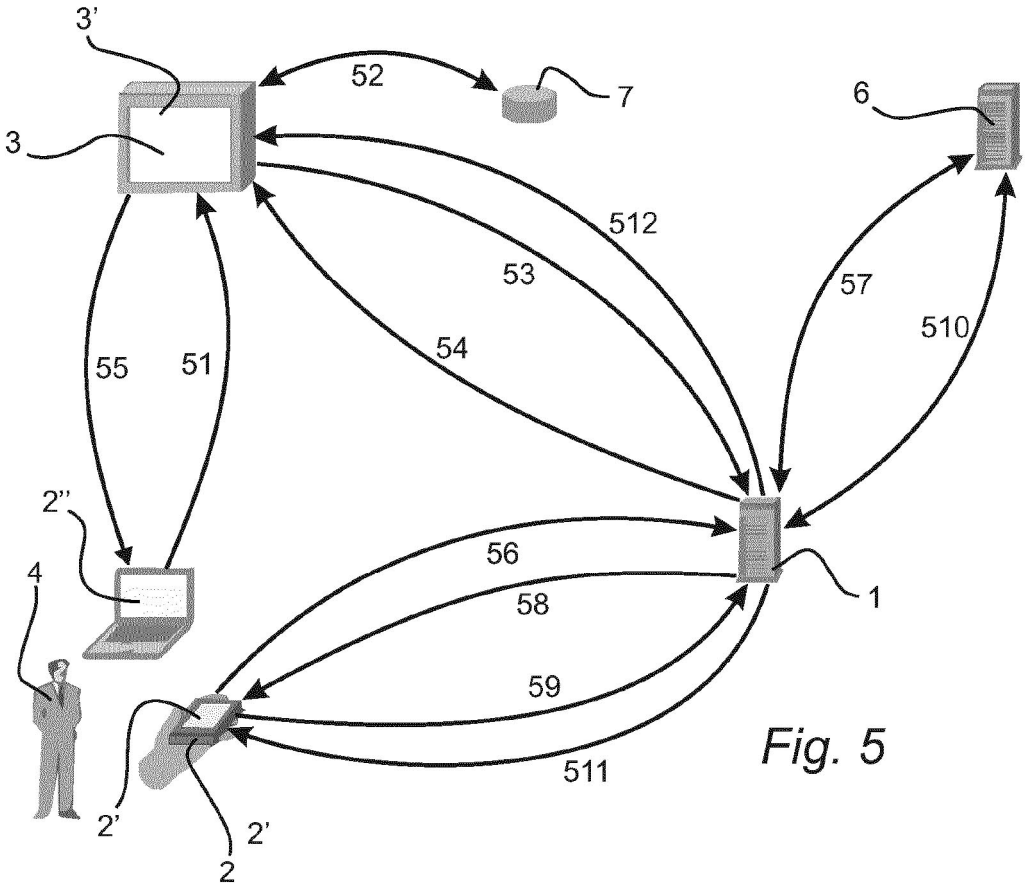
3'
52
7
6
3
512
53
57
510
55
51
54
2''
56
4
58
1
59
511
2'
2'
2

Fig. 5

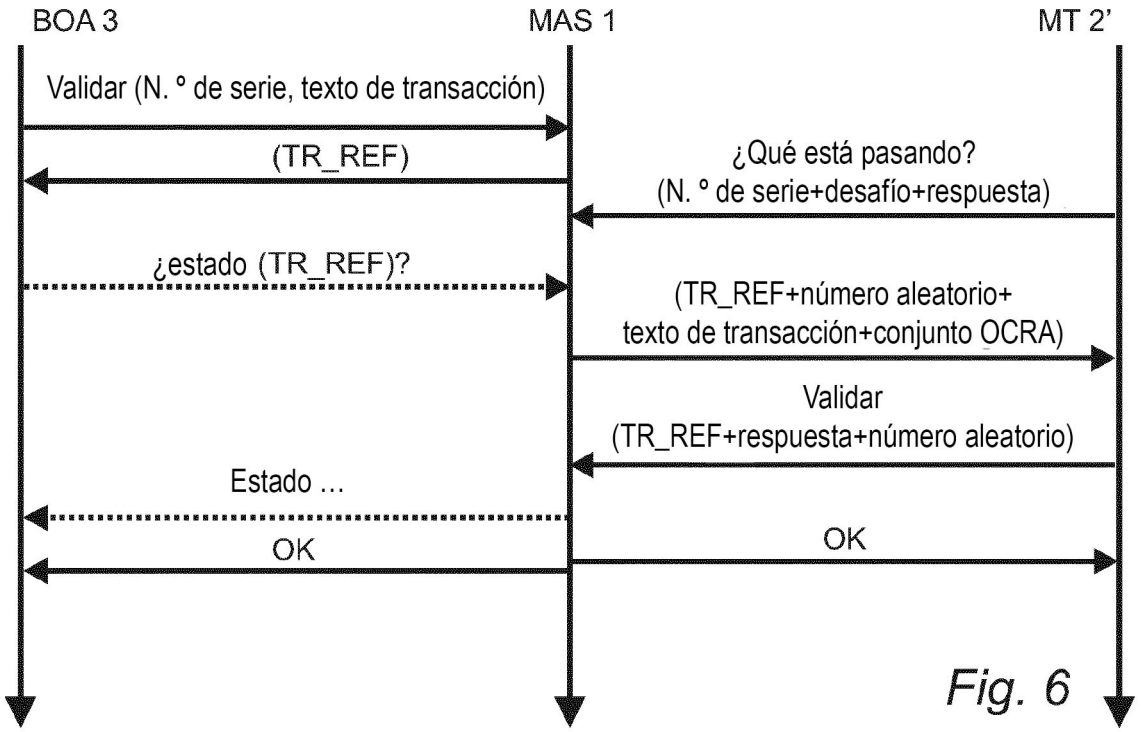
BOA 3
MAS 1
MT 2'
Validar (N. º de serie, texto de transacción)
(TR_REF)
¿Qué está pasando?
(N. º de serie+desafío+respuesta)
¿estado (TR_REF)?
(TR_REF+número aleatorio+
texto de transacción+conjunto OCRA)
Validar
(TR_REF+respuesta+número aleatorio)
Estado ...
OK
OK

Fig. 6