(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 836**

(21) Número de solicitud: 201531491

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 12/08 (2009.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

15.10.2015

(43) Fecha de publicación de la solicitud:

24.04.2017

(71) Solicitantes:

UNIVERSIDAD REY JUAN CARLOS (100.0%)
C/ Tulipán s/n
28933 Móstoles (Madrid) ES

(72) Inventor/es:

BELTRÁN PARDO, Marta y
CARRIEDO SCHER, Francisco

(54) Título: **Procedimiento y sistema para la validación de una petición de autenticación/autorización de un usuario**

(57) Resumen:

Sistema y procedimiento para la validación de una petición de autenticación/autorización de un usuario (EU). Incluye recibir, desde un proveedor de servicios (RP), una petición de autenticación/autorización de un usuario (EU); extraer el contexto dinámico (C) de la petición recibida del proveedor de servicios (RP), donde dicho contexto (C) comprende reglas definidas por el usuario (EU) para su identidad (ID); extraer el perfil (P) asociado a dicha identidad (ID), donde dicho perfil (P) contiene información extraída de contextos históricos asociados a peticiones y transacciones pasadas realizadas para dicha identidad (ID); comprobar el cumplimiento de las reglas incluidas en el contexto (C) por la petición recibida para establecer la validación de dicha petición, y decidir si elevar el nivel de seguridad (LoA) asociado a dicha petición; enviar al proveedor de servicios (RP) información sobre la elevación el nivel de seguridad (LoA).

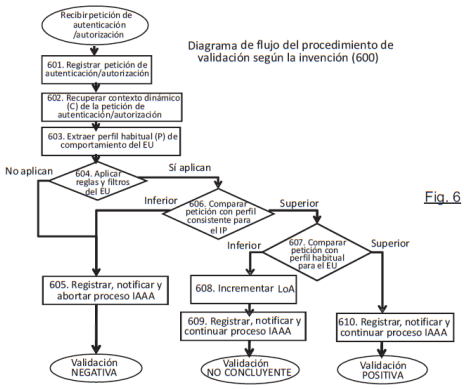

Fig. 6

ES 2 609 836 A1

PROCEDIMIENTO Y SISTEMA PARA LA VALIDACIÓN DE UNA PETICIÓN DE AUTENTICACIÓN/AUTORIZACIÓN DE UN USUARIO

DESCRIPCIÓN

Campo técnico de la invención

La presente invención pertenece al campo de la gestión de identidades digitales.

Antecedentes de la invención o Estado de la Técnica

Previamente se da una pequeña definición de la terminología empleada:

IAAA: Identification, Authentication, Authorization and Accountability. En español: Identificación, Autenticación, Autorización y Trazabilidad.

RP: Relying Party que ofrece algún tipo de activo, recurso, servicio o aplicación y que confía en un proveedor de identidad externo para gestionar los procedimientos IAAA de sus usuarios.

EU: End User o usuario final que desea acceder a los servicios ofrecidos por el RP y utiliza para ello un procedimiento IAAA basado en el número de teléfono y/o en la tarjeta SIM de un terminal (T), es decir, proporcionado por una operadora de telecomunicaciones.

IP: Identity Provider, entidad en la que el usuario realiza el procedimiento IAAA inicialmente. Tanto el RP como el EU confían en esta entidad para atender las peticiones de autenticación y autorización. Para esta invención, se trata de una operadora de telecomunicaciones dado que se tiene en cuenta que la identidad se basa en el número de teléfono y/o en la tarjeta SIM.

Authorization server, Token endpoint y User info endpoint: Sistemas que en la operadora de telecomunicaciones o IP permiten realizar el procedimiento de autenticación mediante OpenIDConnect/MobileConnect, es decir, basando las identidades en el número de teléfono y/o la tarjeta SIM.

LoA: Level of Assurance o nivel de seguridad de un procedimiento IAAA, indica el número y tipo de factores de autenticación que se deben emplear.

Habitualmente, la gestión de identidades digitales se asocia con dos tipos de funcionalidades: la identificación/autenticación y la autorización. Es decir, este tipo de gestión permite, en un contexto digital, verificar que un individuo es quien dice ser pero también autorizar o no, en función de la identidad verificada, el acceso a distintos activos para realizar o no determinadas tareas. Actualmente parece que se ha llegado a un consenso en la industria, según el cual la mejor opción es utilizar soluciones federadas e implantar los esquemas de autenticación sobre los de autorización (especificación OpenIDConnect, que implementa OpenID sobre OAUth).

Además, los esquemas de gestión de identidades digitales han evolucionado hacia el uso de los dispositivos móviles con una tarjeta SIM insertada en el terminal (T) y al número de teléfono asociado a ésta, permitiendo un uso ubicuo de la identidad (especificación MobileConnect basada en OpenIDConnect). Es decir, esquemas que se integren con los dispositivos empleados por los usuarios de manera inteligente, haciendo que los procedimientos de autenticación y autorización no se perciban como procesos diferenciados, complejos y/o costosos, sino que se produzcan de manera natural, sencilla y de la forma más automática y transparente posible para los usuarios. Todo ello manteniendo los niveles de seguridad y control adecuados.

Hay que tener en cuenta que el número de teléfono se asocia cada vez más estrechamente a un individuo concreto que lo mantiene por un largo periodo de tiempo. Además esta asociación suele ser contractual (implicando algún tipo de identificación gubernamental e información bancaria del suscriptor) e involucra a una compañía, la operadora de telecomunicaciones, que es estable, está sujeta a fuertes regulaciones supervisadas por organismos externos nacionales e internacionales y que está obligada a seguir estándares que garanticen la interoperabilidad.

Distintos trabajos están apuntando formas de mejorar la seguridad de estos esquemas basados en OpenIDConnect/MobileConnect añadiendo nuevos factores de autenticación a su modo de operación o convirtiéndolos en más complejos (menos previsibles, más difíciles de adivinar, interceptar y/o generar).

El problema de estas mejoras es que añaden complejidad a los procedimientos IAAA al incrementar los niveles de seguridad, consumiendo recursos en el dispositivo del usuario (batería y ancho de banda de red), obligando a este usuario a tomar parte en el proceso (activando la geo-localización de su dispositivo, fotografiando su cara o escaneando un código QR, por ejemplo) y consumiendo su tiempo y esfuerzo (a veces requiriendo conocimientos técnicos que puede que no tenga), e incurriendo en ocasiones en latencias considerables.

Breve descripción de la invención

Es objeto de la presente invención un procedimiento y un sistema para la validación de una petición.

Respecto del procedimiento para la validación de una petición de autenticación/autorización de un usuario, éste incluye los pasos de: recibir, desde un proveedor de servicios, una petición de autenticación/autorización de un usuario; extraer el contexto dinámico de la petición recibida del proveedor de servicios, donde dicho contexto comprende reglas definidas por el usuario para su identidad; extraer el perfil asociado a dicha identidad, donde dicho perfil contiene información extraída de contextos históricos asociados a peticiones y transacciones pasadas realizadas desde dicha identidad; comprobar el cumplimiento de las reglas incluidas en el contexto por la petición recibida para establecer la validación de dicha petición, y decidir si elevar el nivel de seguridad asociado a dicha petición; enviar al proveedor de servicios información sobre la validación de la petición de autenticación/autorización y sobre la decisión de elevar el nivel de seguridad.

Opcionalmente, la petición de autenticación/autorización del usuario es almacenada para permitir su trazabilidad y para actualizar el perfil asociado a la identidad.

Opcionalmente, un subconjunto de reglas es definido por el usuario.

Opcionalmente, un subconjunto de reglas es definido por la operadora de telecomunicaciones.

Opcionalmente, si el grado de cumplimiento de las reglas definidas por el usuario es inferior a un primer umbral de confianza, la validación es negativa y se finaliza.

Alternativamente, si el grado de cumplimiento de las reglas definidas por el usuario es superior a un primer umbral de confianza, y si el grado de cumplimiento de las reglas definidas por la operadora de telecomunicaciones es inferior a un segundo umbral de confianza, la validación es negativa y se finaliza.

Alternativamente, si el grado de cumplimiento de las reglas definidas por el usuario (EU) es superior a un primer umbral de confianza, y si el grado de cumplimiento de las reglas definidas por la operadora de telecomunicaciones es superior a un segundo umbral de confianza, y si el grado de similitud de la petición de autenticación/autorización con el perfil (P) del usuario (EU) es inferior a un tercer umbral, la validación es no-concluyente y se eleva el nivel de seguridad (LoA) para la

autenticación/autorización posterior. Opcionalmente, en este caso se notifica a la RP el nuevo nivel de seguridad.

Alternativamente, si el grado de cumplimiento de las reglas definidas por el usuario es superior a un primer umbral de confianza, y si el grado de cumplimiento de las reglas definidas por la operadora de telecomunicaciones es superior a un segundo umbral de confianza, y si el grado de similitud de la petición de autenticación/autorización con el perfil del usuario es igual o superior a un tercer umbral, la validación es positiva y se procede directamente con la autenticación/autorización posterior.

Opcionalmente, además se puede enviar al terminal de usuario información sobre la validación de la autenticación/autorización y el nivel de seguridad establecido.

Respecto del sistema para la validación de una petición de autenticación/autorización de un usuario, dicho sistema incluye unos medios de recepción para recibir y registrar una petición de autenticación/autorización lanzada por un proveedor de servicios en respuesta a un procedimiento iniciado por un usuario desde un dispositivo; unos medios de extracción para extraer el contexto dinámico de la petición recibida, donde dicho contexto comprende reglas y filtros definidos por el usuario para su identidad; unos medios de comprobación para validar la petición recibida por los medios de recepción frente a su contexto dinámico y el perfil obtenido de los medios de extracción, adecuando el nivel de seguridad del posterior procedimiento de autenticación / autorización en función del resultado de la validación.

Ventajosamente, la presente invención permite validar una petición de autenticación/autorización basada en el número de teléfono y/o en la tarjeta SIM antes de realizar el procedimiento completo de autenticación/autorización. Se consigue mejorar la seguridad y la eficiencia en el uso de los recursos, tanto el usuario (EU) como de la operadora de telecomunicaciones (IP), de manera que en el caso de peticiones no validadas (clasificadas como inseguras), ni siquiera se intente realizar el procedimiento de autenticación/autorización. Esto se explica más detalladamente a continuación.

En caso de que el resultado de validación previa sea positivo, se pasa a realizar el procedimiento de autenticación/autorización con el esquema que se estuviera utilizando por parte de la operadora de telecomunicaciones (p.e. OpenIDConnect/MobileConnect).

En caso de que el resultado de validación previa sea negativo, se evita continuar con el procedimiento de autenticación/autorización y se ignora la petición recibida. Con

ello, se evita el consumo de recursos en el dispositivo, de tiempo y esfuerzo por parte del usuario y la latencia asociada.

En caso de que el resultado de validación previa sea no concluyente, se incrementa el nivel de seguridad de la posterior autenticación/autorización al resultar la petición dudosa o sospechosa (es decir, si se decide que el procedimiento de autenticación/autorización continúe, pero hay sospechas acerca de su origen, consistencia y legitimidad, se aumenta el LoA).

Se propone un MID proxy que se disponga delante de los sistemas que realizan la autenticación/autorización en las operadoras de telecomunicaciones para llevar a cabo la validación propuesta sin necesidad de modificar o alterar estos sistemas y los procedimientos de autenticación que ya estuvieran usando (p.e. OpenIDConnect/MobileConnect).

Ventajosamente la validación propuesta no precisa que el usuario instale ningún tipo de aplicación en su dispositivo móvil. Basta con contratar el servicio asociado con su operadora. Este servicio se denomina MIDaaS (Mobiquitous Identity as a Service) de aquí en adelante.

El procedimiento de validación de las peticiones de autenticación/autorización se basa en dos aspectos fundamentales:

Trazabilidad: La monitorización en tiempo real y registro de actividad de todas las transacciones llevadas a cabo con una identidad digital, de manera que se almacene un registro completo de todas ellas del que se pueda extraer el patrón de comportamiento considerado habitual para esa identidad (perfil del EU). Algunos de los atributos que caracterizan este patrón (aunque se pueden añadir tantos como se desee) son: RP origen de la petición de autenticación, información asociada a esta RP (tipo de activo, recurso, servicio o aplicación ofrecida, sector de actividad, nombre de dominio, localización geográfica/idioma, dirección IP, etc.), hora de la petición de autenticación, tiempo de expiración especificado, LoA requerido (nivel de seguridad), geo-localización del dispositivo del EU, información adicional acerca del EU asociada a esta petición (dispositivo de acceso, red de acceso, dirección IP, etc.) y resultado del procedimiento de validación.

El contexto dinámico de la petición: Toda aquella información acerca de la petición que pueda ayudar a la operadora de telecomunicaciones a realizar la validación de la petición de autenticación/autorización antes de tener que procesarla. Estos atributos son, para cada petición en particular, muy similares a los que quedan registrados en el

patrón asociado a cada identidad, por lo tanto RP origen de la petición de autenticación, información asociada a esta RP, hora de la petición de autenticación, tiempo de expiración especificado, LoA requerido, geo-localización del dispositivo del EU, información adicional acerca del EU.

Además, este contexto incluye también reglas o filtros dinámicos especificados por el propio usuario en cada momento o caso. Por ejemplo, el contexto de una petición de autenticación puede incluir un filtro que el EU ha activado para indicar que no se procesen peticiones de autenticación para redes sociales entre las 23.00 y las 7.00. O que no se procesen peticiones de autenticación para sitios de comercio electrónico con dominio .cn.

Breve descripción de las figuras

Figura 1: Flujo según el estado de la técnica anterior para añadir identificación/ autenticación a una autorización (OpenIDConnect/MobileConnect).

Figura 2: Flujo de acuerdo con la invención cuando el resultado de la validación es positivo.

Figura 3: Flujo acuerdo con la invención cuando el resultado de la validación es no concluyente.

Figura 4: Flujo acuerdo con la invención cuando el resultado de la validación es negativo.

Figura 5: Detalle del paso 3 de las figuras 2 a 4 con el flujo de validación realizado por el MID proxy de acuerdo con la invención.

Figura 6: Diagrama de flujo del procedimiento de validación según la invención.

Figura 7: Diagrama de bloques según la invención para el MID proxy.

Descripción detallada de la invención

Con fines aclaratorios y haciendo referencia a las figuras anteriores, se exponen varios ejemplos de realización. Estos ejemplos no tienen carácter restrictivo sobre el alcance de la presente invención.

La **figura 1** muestra el esquema conocido en un caso de uso básico según una técnica actual (OpenIDConect 1.0/MobileConnect sobre OAuth 2.0). De esta forma, se permite que una RP verifique la identidad de un usuario mediante un procedimiento de

autenticación/autorización realizado por el propio Authorization Server, así como obtener información básica asociada a su perfil (nombre, apellidos, email, etc.). Como se puede observar se añade al Access Token empleado por OAuth para gestionar la autorización un ID Token para poder realizar la autenticación. Gracias a este esquema, las operadoras de telecomunicaciones se pueden convertir en proveedoras de identidad basada en el número de teléfono y/o en la tarjeta SIM. Para incrementar el nivel de seguridad del procedimiento IAAA, se podrían añadir nuevos factores de autenticación que requieran de la intervención activa del usuario obligando a este usuario a tomar parte en el proceso (activando la geo-localización de su dispositivo, fotografiando su cara o escaneando un código QR, por ejemplo). Todos ellos consumen además recursos en el dispositivo del usuario (batería y ancho de banda de red), por lo que quedan seriamente restringidos los escenarios en los que se pueden emplear.

En la **figuras 2-4** se puede ver un diagrama de flujo con diferentes pasos. A continuación, se pasa a comentar cada uno.

Paso 1: La RP crea la petición de autenticación/autorización para realizar procedimiento IAAA con el EU (normalmente porque el EU habrá solicitado desde algún dispositivo, acceder a un activo, recurso, aplicación o servicio que provee la RP previamente).

Paso 2: La RP lanza esta petición de autenticación/autorización al MID proxy en el IP.

Paso 3: Este proxy realiza el procedimiento de validación objeto de esta invención (descrito más adelante en detalle), y tras esta validación, la registra junto con su resultado para llevar una traza de los eventos asociados a la identidad del EU y la envía al Authorization Server.

Paso 4: Lo que ocurre a continuación depende del resultado del procedimiento de validación:

Opción 4.1: Si el resultado de la validación ha sido positivo, el MIDProxy permite que el procedimiento IAAA comience normalmente, re-enviando la petición de autenticación/autorización al Authorization Server. Esto se muestra en la **figura 2**.

Opción 4.2: Si el resultado de la validación ha sido no concluyente, el MIDProxy incrementa el Level of Assurance (LoA) antes de permitir que comience el procedimiento IAAA, re-enviando la petición de autenticación/autorización al Authorization Server. También notifica al RP el nuevo valor del LoA para que el posterior procedimiento de autenticación/autorización se lleve a cabo sin problemas. Esto se muestra en la **figura 3**.

Opción 4.3: Si el resultado de la validación ha sido negativo, simplemente notifica al EU y la RP y no se llega a realizar el procedimiento IAAA que queda abortado (aunque registrado para posteriores comprobaciones). Esto se muestra en la **figura 4**.

Paso 5: En las dos primeras opciones (4.1 y 4.2), el procedimiento IAAA continúa con normalidad por lo que el EU proporciona su consentimiento para este proceso al MID proxy.

Paso 6: El MID proxy registra el consentimiento y lo envía al Authorization Server.

Paso 7: El Authorization server genera un código de autorización para el EU y se lo envía al MID proxy para que quede registrado.

Paso 8: El MID proxy se lo hace llegar al EU.

Paso 9: El EU presenta este código de autorización a la RP.

Paso 10: La RP presenta este código de autorización en el Token endpoint del IP para obtener los token de acceso e identidad (Access Token e ID Token respectivamente).

Paso 11: El Token endpoint envía estos tokens a la RP.

Paso 12: La RP valida el ID Token, con lo que el procedimiento de autenticación/autorización se da por finalizado y el EU puede acceder a los recursos que había solicitado inicialmente, quedando todo el procedimiento IAAA registrado en el MID proxy.

Paso 13: Opcionalmente la RP puede utilizar el Access Token para dirigirse al MID proxy y solicitar información adicional sobre el EU, estática (User Info) o dinámica (Context).

Paso 14: Esta petición se registra en el MID proxy y se re-dirige al User Info + Context endpoint.

Paso 15: Este endpoint responde al MID proxy con la información solicitada.

Paso 16: El MID proxy registra esta respuesta y la re-dirige a la RP.

La **figura 5** especifica en detalle el flujo del procedimiento de validación realizado por el MID proxy y que se ha resumido como "validación y registro" en el paso 3 de las figuras 2, 3 y 4.

Como se puede ver este proxy se encarga de realizar el procedimiento de validación, por lo que reúne en sí tres cometidos principales característicos del esquema propuesto en esta invención:

1. Realizar el registro de transacciones que contiene datos sobre toda acción que se produzca relativa a la identidad de un EU, lo cual permite ofrecer trazabilidad tanto al EU (de su identidad) como a la RP (de las identidades de todos sus usuarios). El “Registro de transacciones” es el elemento que almacena los datos asociados a todas las peticiones (todos los atributos de las peticiones de autenticación/autorización que

ya se han enumerado), independientemente de su resultado final y que permite a otros módulos o componentes resumir en un patrón de comportamiento habitual lo que se considera “normal” para una identidad concreta. La extracción de características para resumir este patrón se puede realizar con cualquiera de los métodos y algoritmos tradicionales que se emplean en reconocimiento de patrones.

2. Obtener el contexto de la petición, atendiendo a los factores dinámicos que se consideren oportunos, tanto para el EU como para la RP, en base a los cuales se puede discriminar entre peticiones consistentes y no consistentes, es decir, entre peticiones que se consideran seguras y se validan porque se pueden completar con éxito o peticiones, dudosas (en las que se incrementa el nivel de seguridad necesario en la posterior autenticación) o del todo inseguras (que se abortan). El “Servidor de contexto” es el elemento encargado de enriquecer la petición con toda la información de contexto relevante (también mencionada con anterioridad), y esto incluye las reglas o filtros que se permite que definan los propios EU en relación con sus identidades.

3. Contrastar la petición enriquecida con los criterios personales establecidos por el EU y con criterios generales de validación (aquellos que toda deben petición debe cumplir para resultar consistente).

a. Criterios personales de validación: Es necesario comprobar si en el contexto de la petición se incorpora alguna regla o filtro de las especificadas por el EU. Como ejemplo de criterio personal de validación, una petición proveniente de un determinado nombre de dominio, en determinada franja horaria o solicitando determinada autorización para determinado tipo de activos, recursos, servicios o aplicaciones puede ser desestimada directamente por lo que el resultado de la validación ya sería negativo.

b. Criterios generales de validación: Si se pasan los criterios personales de validación es necesario aplicar los generales.

Primero se aplican criterios de validación general especificados por el IP para distinguir entre peticiones consistentes y no consistentes. Como ejemplo de criterio general de validación, una petición que de momento está catalogada como consistente (no está afectada por ninguna regla del EU) pero en la que la localización del servicio RP afirma la posición del dispositivo de acceso del EU está en Roma, mientras que la localización independiente del EU revela que su dispositivo móvil se encuentra en Londres (la máquina con la que se navega el sitio web de la RP y el terminal móvil pueden ser independientes, pero deben encontrarse físicamente próximos a no ser que se indique lo contrario), terminaría con un resultado negativo para la validación. Por último, si se han cumplido con éxito todos los criterios anteriores, una vez

extraídas las características de la petición de autenticación/autorización y de su contexto (con los atributos ya mencionados), se pueden comparar con el patrón de comportamiento considerado habitual para esa identidad digital (perfil del EU).

i. Con un nivel de coincidencia suficiente, se finaliza con una validación positiva. El umbral para el nivel de coincidencia dependerá del nivel de seguridad requerido por cada usuario.

ii. Con un nivel de coincidencia por debajo de este umbral, se permite realizar el procedimiento de autenticación/autorización pero se aumenta su nivel de seguridad, es decir, el LoA (resultado de la validación no concluyente, como hay dudas o sospechas, se continúa con el procedimiento IAAA pero aumentando los requisitos de seguridad).

EJEMPLO 1

En este ejemplo un EU que dispone del servicio MIDaaS activado visita desde su ordenador portátil un sitio web de un RP que ofrece un servicio en el que está interesado. Como es usual, el sitio web requiere que el EU se identifique y autentique antes de poder acceder al servicio.

El EU escoge Autenticarse a través del IP (facilitando simplemente su número de teléfono), obteniendo la RP los datos personales y de contexto del EU que éste la autoriza a obtener sin necesidad de que el EU introduzca ninguna otra información.

Supongamos cuatro escenarios:

1. La petición de autenticación/autorización del RP para este EU se registra en el MID Proxy. A continuación, se recupera el contexto de esta petición. Ningún criterio personal del EU hace sospechar que se trate de una petición no consistente. Tampoco hay problema con los criterios generales de validación: la petición entra dentro del patrón de comportamiento normal del EU (ya había utilizado antes los servicios de este RP en un horario y localización similar) y no hay ningún otro particular de relevancia. El resultado de la validación es positivo y se procede a autenticar al usuario con el LoA requerido inicialmente. El EU se autentica con éxito.

2. La petición de autenticación/autorización del RP para este EU se registra en el MID Proxy. A continuación, se recupera el contexto de esta petición. Ningún criterio personal del EU hace sospechar que se trate de una petición no consistente. Surge una sospecha al aplicar los criterios generales: la petición no entra en absoluto dentro del patrón de comportamiento normal del EU: nunca había utilizado los servicios de este RP, no suele acceder a este tipo de servicios en este horario, se trata de un dominio en una zona geográfica poco habitual, etc. El resultado de la validación es no

concluyente y se procede a autenticar al usuario con un LoA superior al requerido inicialmente, por lo que son necesarios más factores de autenticación de los que se habrían empleado con normalidad. El EU se autentica con éxito y se actualiza su patrón de comportamiento habitual con esta petición. Si el EU no consiguiera finalizar el procedimiento de autenticación/autorización con éxito, se habría evitado una suplantación de identidad al detectar una petición que no encaja con el perfil de comportamiento habitual del usuario.

3. La petición de autenticación/autorización del RP para este EU se registra en el MID Proxy. A continuación, se recupera el contexto de esta petición. Ningún criterio personal del EU hace sospechar que se trate de una petición no consistente. Surge una sospecha al aplicar los criterios generales: la distancia entre el dispositivo (un ordenador o una tableta, por ejemplo) utilizado por el EU para acceder al RP y su terminal móvil (aquel que contiene la tarjeta SIM) es de cientos de kilómetros (y el EU no ha actualizado sus criterios de validación personal para avisar de este particular). La validación tiene un resultado negativo y ni siquiera se lanza el procedimiento de autenticación/autorización. Se ha evitado una posible suplantación de identidad, al no cumplirse un criterio que considerado imprescindible para catalogar la petición como consistente. Todo queda registrado de manera que tanto el IP como el EU puedan analizar el caso posteriormente y tomar las acciones necesarias.

4. La petición de autenticación/autorización del RP para este EU se registra en el MID Proxy. A continuación, se recupera el contexto de esta petición. Se detecta un criterio personal del EU que permite catalogar la petición como no consistente inmediatamente: no se permite realizar autenticaciones para este tipo de servicio en esta franja horaria. La validación tiene un resultado negativo y ni siquiera se lanza el procedimiento de autenticación/autorización. Se ha evitado una posible suplantación de identidad. Todo queda registrado de manera que se pueda analizar el caso posteriormente y tomar las acciones necesarias.

EJEMPLO 2

Hace años que existen operadoras de telecomunicaciones que ofrecen la posibilidad de realizar pagos a través de los terminales móviles y de las operadoras, sin necesidad alguna de ningún otro elemento. Esta práctica, se suele denominar telco-billing y permite que un suscriptor de telefonía móvil cargue sus compras a su cuenta a través de su operadora de telecomunicaciones.

En este ejemplo una empresa permite a sus empleados (EU) realizar pagos mediante su terminal móvil corporativo para evitar el manejo de tarjetas bancarias de empresa.

Supongamos que uno de estos empleados intenta realizar un pago por móvil en un establecimiento (RP) dentro de su horario laboral, en el ámbito geográfico de su oficina y por un importe autorizado por su compañía. La petición de autenticación/autorización del RP para este EU se registra en el MID Proxy. A continuación, se recupera el contexto de esta petición. Ningún criterio personal del EU (en este caso estos criterios los fija su empresa, que es la que tiene contratada la línea) hace sospechar que se trate de una petición no consistente. Tampoco hay problema con los criterios generales de validación: la petición entra dentro del patrón de comportamiento normal del EU (ya había utilizado antes los servicios de este RP en un horario y localización similar) y no hay ningún otro particular de relevancia. El resultado de la validación es positivo y se procede a autenticar al usuario con el LoA requerido inicialmente. El EU se autentica con éxito y se autoriza el pago.

Ahora supongamos un segundo escenario en el que el empleado ha extraviado su dispositivo móvil o se lo han robado. Supongamos además que tenía apuntadas todas sus contraseñas en un archivo almacenado en el dispositivo. Si una persona en posesión del dispositivo y de las contraseñas intenta realizar un pago antes de que la empresa anule la tarjeta SIM del dispositivo, sucedería lo siguiente: la petición de autenticación/autorización del RP para este EU falso se registra en el MID Proxy. A continuación, se recupera el contexto de esta petición.

En primer lugar si el pago no está dentro del horario, ámbito geográfico o importe autorizados por la compañía a través de los criterios personales de validación, la petición de autenticación/autorización no se procesará y se habrá evitado una suplantación de la identidad. Si estos criterios no clasifican a la petición como no consistente, probablemente los de validación general (por salirse el pago del patrón de comportamiento normal del EU o el resto de criterios que apliquen) la pasen a no consistente, abortándola o como mínimo, aumentando el LoA y así, ni siquiera realizando la autenticación/autorización o realizándola con mayor número de factores de autenticación (es decir, con una probabilidad mucho mayor de evitar la suplantación).

En la **figura 6** se puede observar un diagrama de flujo del procedimiento de validación según la invención (600). El procedimiento comienza al recibir la petición de autenticación/autorización lanzada por un RP (en respuesta a una solicitud de servicio del usuario). A continuación, se registra la petición de autenticación/autorización (601) y en un siguiente paso, se recupera el contexto dinámico (C) de esta petición (602). Después se extrae el perfil habitual (P) de comportamiento del EU involucrado en el procedimiento IAAA que se desea iniciar con esta petición recibida (603).

En el siguiente paso (604), se aplican las reglas y filtros del EU que se recuperaron con el contexto C. Si no se pasa esta aplicación porque no se cumple con alguna de estas reglas o filtros, se procederá a registrar este resultado, notificarlo a las partes y a abortar el procedimiento IAAA (605). El resultado de la validación será directamente NEGATIVO.

Si se pasan los criterios personales de validación para el usuario, a continuación se compara la petición recibida con lo que se considera un perfil consistente para el IP (606). Es decir, se aplican los criterios generales de validación de la operadora para cualquier petición. Si no se cumplen estos criterios y la similitud con el perfil deseado está por debajo de un umbral, se procederá a registrar este resultado, notificarlo a las partes y a abortar el procedimiento IAAA (605). El resultado de la validación será directamente NEGATIVO.

Si se pasan estos criterios, se procede a comparar la petición recibida con perfil habitual para el EU, P (607). Si la similitud con este perfil habitual está por debajo de un umbral, se procederá a incrementar el nivel de seguridad del posterior procedimiento de autenticación/autorización (608) y a registrar este resultado, notificarlo a las partes y a continuar el procedimiento IAAA (609). El resultado de la validación será NO CONCLUYENTE. Si por el contrario está por encima de este umbral, se procederá a registrar este resultado, notificarlo a las partes y a continuar el procedimiento IAAA (610) tal y como se había solicitado desde el principio (sin modificar el LoA). El resultado de la validación será POSITIVO.

Un ejemplo de realización como sistema (70) se ilustra en la **figura 7**. En los diferentes bloques funcionales se ilustran posibles módulos de implementación.

En particular, se puede observar un medio de recepción (71) que recibe, desde un proveedor de servicios (RP) una petición de autenticación/autorización realizada a través de un dispositivo (D) que puede ser por ejemplo un ordenador de sobremesa, una tableta o un portátil y la incluye en un registro histórico de transacciones. Esto corresponde con el bloque 601 del diagrama de flujo 600.

También es necesario un medio de extracción (72) que recupere toda la información que constituye el contexto de la petición (C) y que se va a emplear en la posterior validación. Por lo tanto, el contexto de la propia petición recibida desde el RP, el contexto del EU (por medio de la identidad empleada en su relación con el RP) y las reglas y filtros que este usuario define para que se apliquen sus criterios de validación personal. Esto corresponde con el bloque 602 del diagrama de flujo 600.

Por último, el medio de comprobación (73) recibe la petición de autorización/autenticación y su contexto C y procede a evaluarlos (bloques del 603 en

adelante para el diagrama de flujo 600). Este medio es capaz de generar un perfil habitual de comportamiento (P) para el usuario a partir de la información almacenada el registro histórico de transacciones. Aplicando a la petición y contexto recibidos las reglas y filtros incluidos en el propio contexto y comparando sus características con este perfil habitual de comportamiento, este medio comprueba si la petición recibida puede seguir adelante, si se debe incrementar su nivel de seguridad (LoA) o si se debe abortar.

REIVINDICACIONES

1. Procedimiento para la validación de una petición de autenticación/autorización de un usuario (EU) caracterizado por que comprende:

- recibir, desde un proveedor de servicios (RP), una petición de autenticación/autorización de un usuario (EU);
- extraer el contexto dinámico (C) de la petición recibida del proveedor de servicios (RP), donde dicho contexto (C) comprende reglas definidas por el usuario (EU) para su identidad (ID);
- extraer el perfil (P) asociado a dicha identidad (ID), donde dicho perfil (P) contiene información extraída de contextos históricos asociados a peticiones y transacciones pasadas realizadas desde dicha identidad (ID);
- comprobar el cumplimiento de las reglas incluidas en el contexto (C) por la petición recibida para establecer la validación de dicha petición, y decidir si elevar el nivel de seguridad (LoA) asociado a dicha petición;
- enviar al proveedor de servicios (RP) información sobre la validación de la petición de autenticación/autorización y sobre la decisión de elevar el nivel de seguridad (LoA).

2. Procedimiento según la reivindicación 1, caracterizado por que la petición de autenticación/autorización del usuario (EU) es almacenada para permitir su trazabilidad y para actualizar el perfil (P) asociado a la identidad (ID).

3. Procedimiento según la reivindicación 1 o 2, caracterizado por que un subconjunto de reglas es definido por el usuario (EU).

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que un subconjunto de reglas es definido por la operadora de comunicaciones (IP).

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que si el grado de cumplimiento de las reglas definidas por el usuario (EU) es inferior a un primer umbral de confianza, la validación es negativa y se finaliza.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que:

- si el grado de cumplimiento de las reglas definidas por el usuario (EU) es superior a un primer umbral de confianza, y

- si el grado de cumplimiento de las reglas definidas por la operadora de comunicaciones (IP) es inferior a un segundo umbral de confianza, la validación es negativa y se finaliza.

7. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que:
- si el grado de cumplimiento de las reglas definidas por el usuario (EU) es superior a un primer umbral de confianza, y
- si el grado de cumplimiento de las reglas definidas por la operadora de comunicaciones (IP) es superior a un segundo umbral de confianza, y
- si el grado de similitud de la petición de autenticación/autorización con el perfil (P) del usuario (EU) es inferior a un tercer umbral, la validación es no-concluyente y se eleva el nivel de seguridad (LoA) para la autenticación/autorización posterior.

8. Procedimiento según la reivindicación 7, caracterizado por que se notifica a la RP el nuevo nivel de seguridad (LoA).

9. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que:
- si el grado de cumplimiento de las reglas definidas por el usuario (EU) es superior a un primer umbral de confianza, y
- si el grado de cumplimiento de las reglas definidas por la operadora de comunicaciones (IP) es superior a un segundo umbral de confianza, y
- si el grado de similitud de la petición de autenticación/autorización con el perfil (P) del usuario (EU) es igual o superior a un tercer umbral, la validación es positiva y se procede directamente con la autenticación/autorización posterior.

10. Procedimiento según una cualquiera de las reivindicaciones 1 a 9, caracterizado por que comprende además enviar al terminal de usuario (T) información sobre la validación de la autenticación/autorización y el nivel de seguridad (LoA) establecido.

11. Sistema (70) para la validación de una petición de autenticación/autorización de un usuario (EU) caracterizado por que comprende:
- medios de recepción (71) configurados para recibir y registrar una petición de autenticación / autorización lanzada por un proveedor de servicios (RP) en respuesta a un procedimiento iniciado por un usuario desde un dispositivo (D);

- medios de extracción (72) configurados para extraer el contexto dinámico (C) de la petición recibida, donde dicho contexto (C) comprende reglas y filtros definidos por el usuario para su identidad (ID);

- medios de comprobación (73) configurados para validar la petición recibida por los medios de recepción (71) frente a su contexto dinámico (C) y del perfil (P) obtenido de los medios de extracción (72), adecuando el nivel de seguridad (LoA) del posterior procedimiento de autenticación / autorización en función del resultado de la validación.

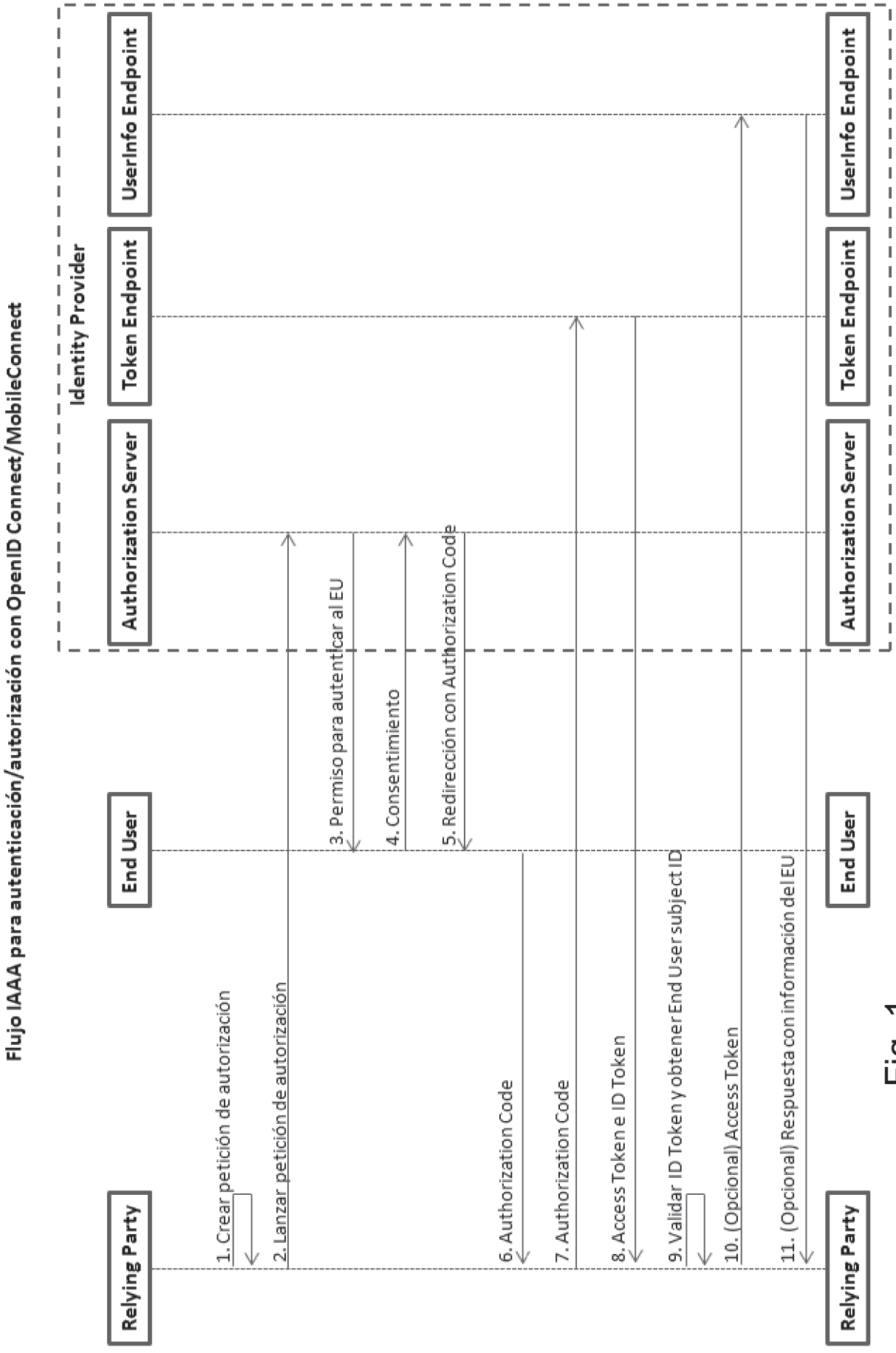
Flujo IAAA para autenticación/autorización con OpenID Connect/MobileConnect
Identity Provider
Relying Party
End User
Authorization Server
Token Endpoint
UserInfo Endpoint
1. Crear petición de autorización
2. Lanzar petición de autorización
3. Permiso para autenticar al EU
4. Consentimiento
5. Redirección con Authorization Code
6. Authorization Code
7. Authorization Code
8. Access Token e ID Token
9. Validar ID Token y obtener End User subject ID
10. (Opcional) Access Token
11. (Opcional) Respuesta con información del EU

Fig. 1

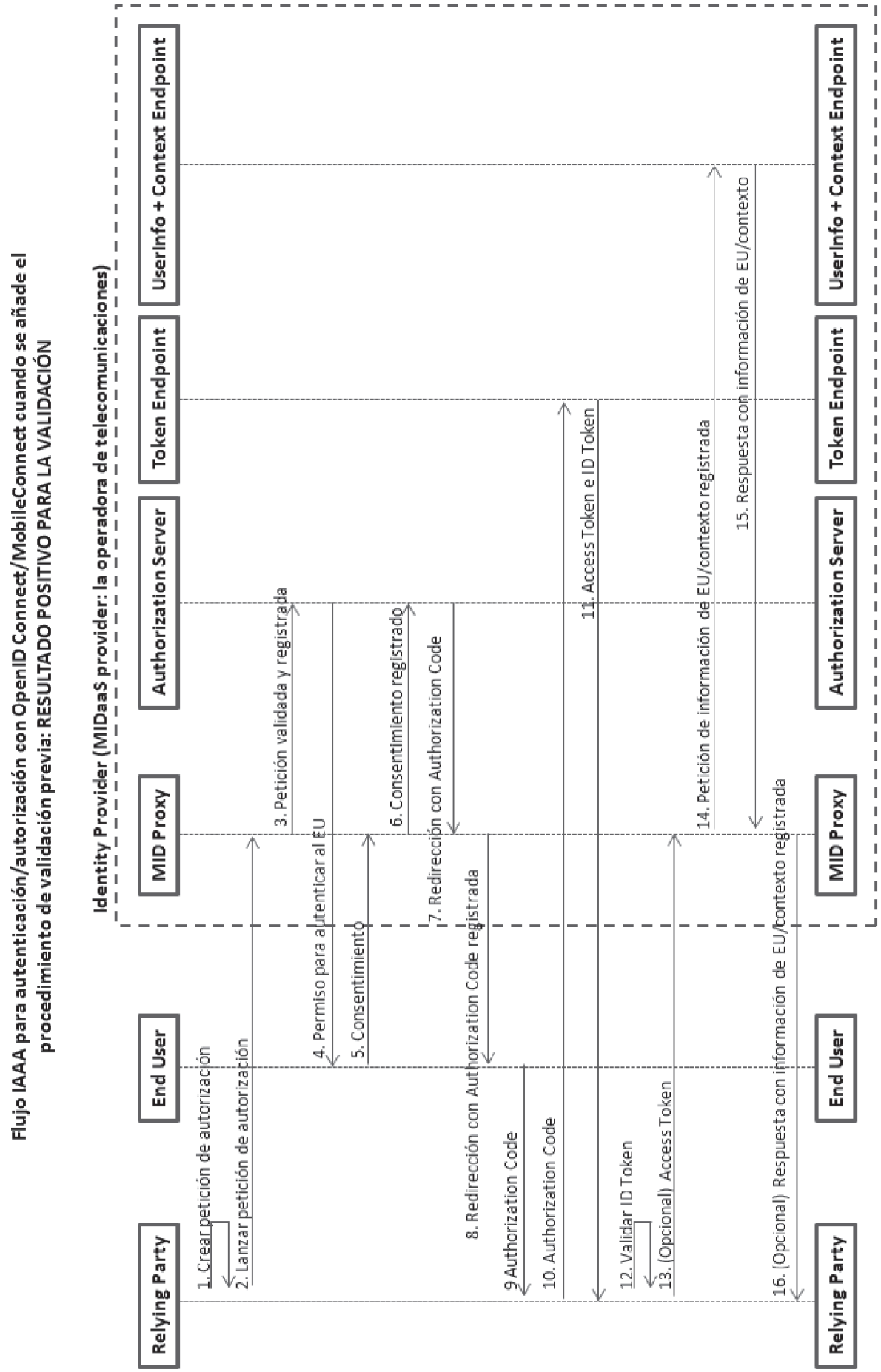
Flujo IAAA para autenticación/autorización con OpenID Connect/MobileConnect cuando se añade el procedimiento de validación previa: RESULTADO POSITIVO PARA LA VALIDACIÓN
Identity Provider (MIDaaS provider: la operadora de telecomunicaciones)
Relying Party
End User
MID Proxy
Authorization Server
Token Endpoint
UserInfo + Context Endpoint
1. Crear petición de autorización
2. Lanzar petición de autorización
3. Petición validada y registrada
4. Permiso para autenticar al EU
5. Consentimiento
6. Consentimiento registrado
7. Redirección con Authorization Code
8. Redirección con Authorization Code registrada
9 Authorization Code
10. Authorization Code
11. Access Token e ID Token
12. Validar ID Token
13. (Opcional) Access Token
14. Petición de información de EU/contexto registrada
15. Respuesta con información de EU/contexto
16. (Opcional) Respuesta con información de EU/contexto registrada

Fig. 2

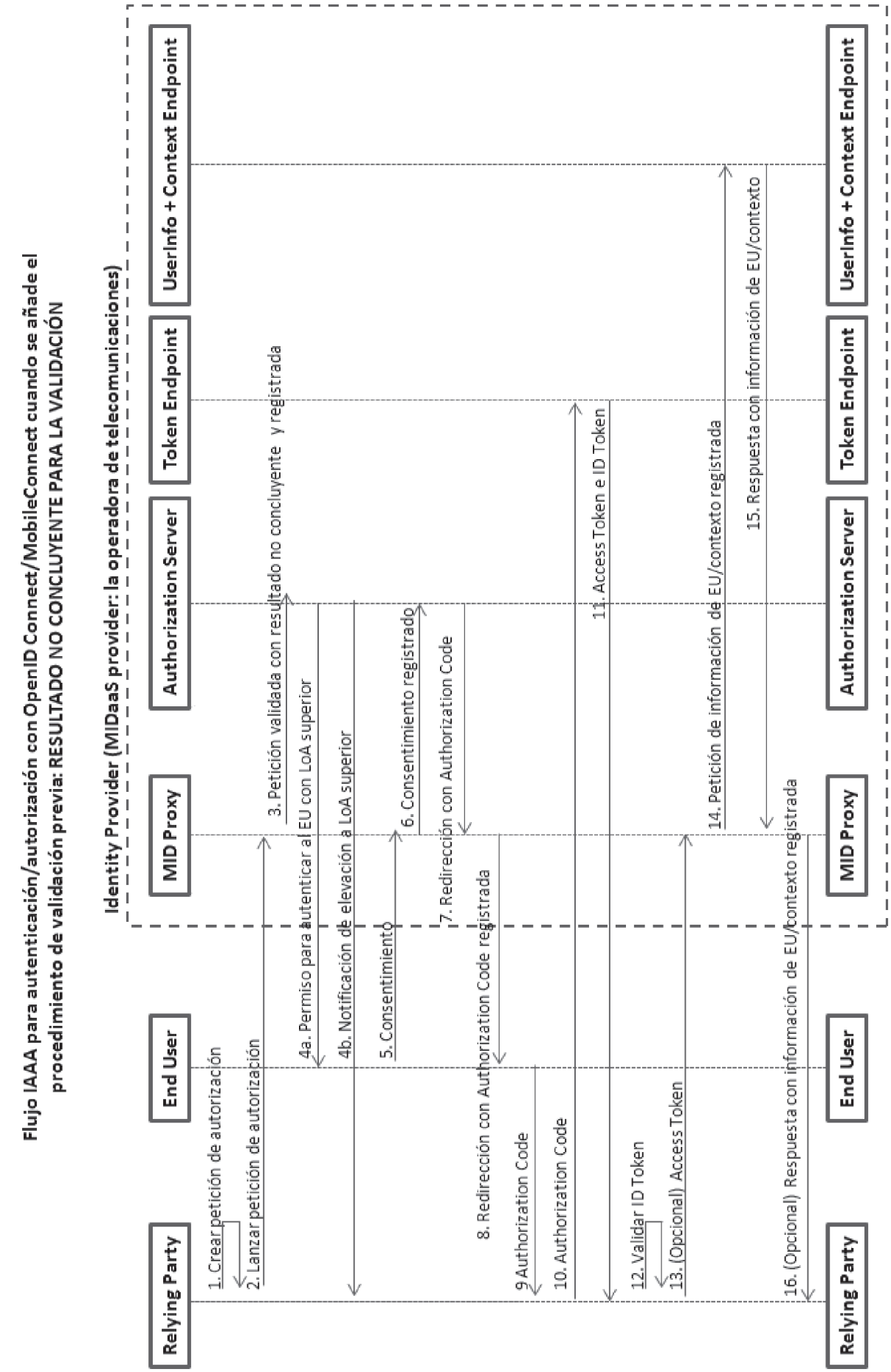
Flujo IAAA para autenticación/autorización con OpenID Connect/MobileConnect cuando se añade el procedimiento de validación previa: RESULTADO NO CONCLUYENTE PARA LA VALIDACIÓN
Identity Provider (MIDaaS provider: la operadora de telecomunicaciones)
Relying Party
End User
MID Proxy
Authorization Server
Token Endpoint
UserInfo + Context Endpoint
1. Crear petición de autorización
2. Lanzar petición de autorización
3. Petición validada con resultado no concluyente y registrada
4a. Permiso para autenticar al EU con LoA superior
4b. Notificación de elevación a LoA superior
5. Consentimiento
6. Consentimiento registrado
7. Redirección con Authorization Code
8. Redirección con Authorization Code registrada
9 Authorization Code
10. Authorization Code
11. Access Token e ID Token
12. Validar ID Token
13. (Opcional) Access Token
14. Petición de información de EU/contexto registrada
15. Respuesta con información de EU/contexto
16. (Opcional) Respuesta con información de EU/contexto registrada

Fig. 3

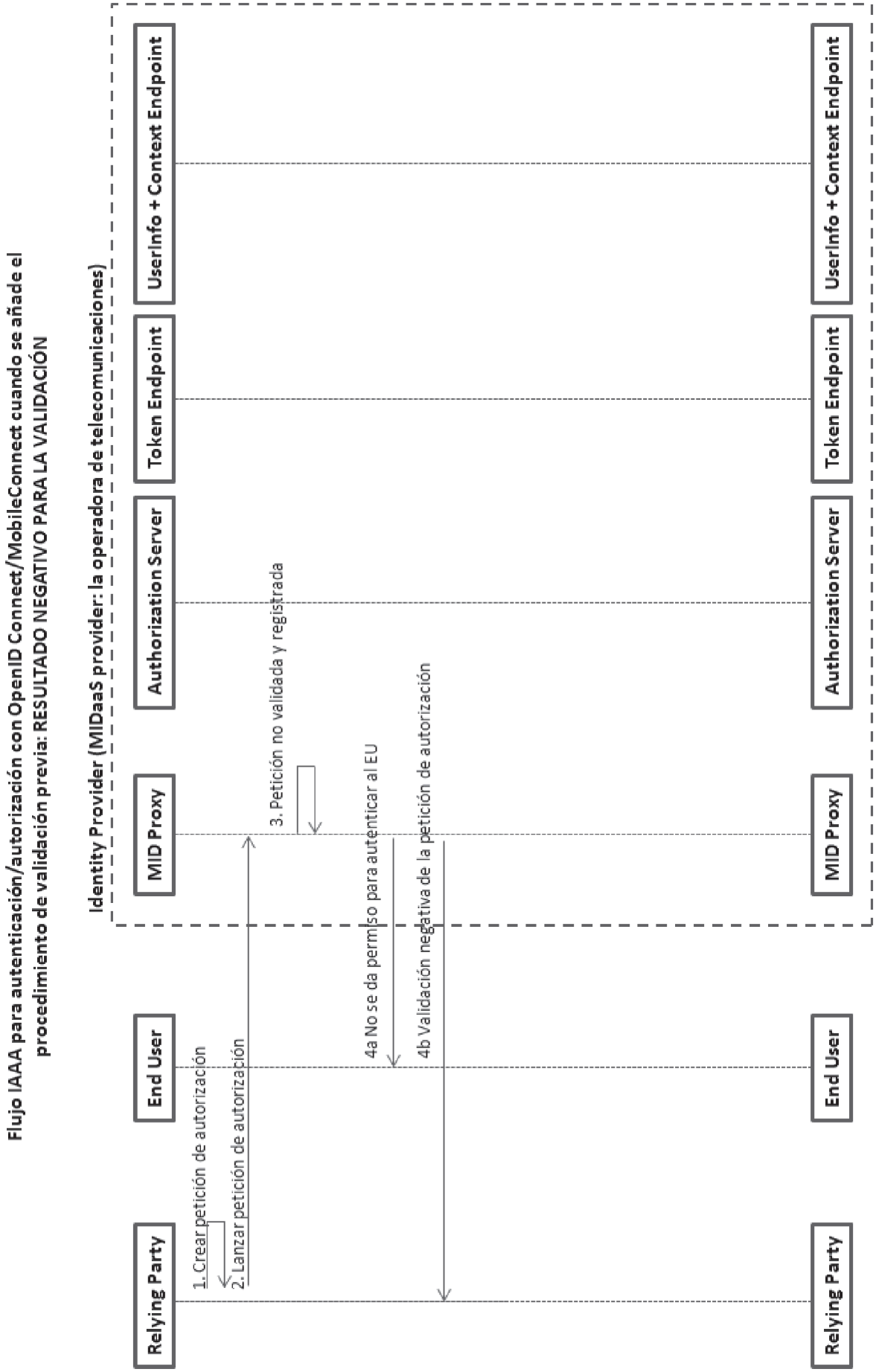
Flujo IAAA para autenticación/autorización con OpenID Connect/MobileConnect cuando se añade el procedimiento de validación previa: RESULTADO NEGATIVO PARA LA VALIDACIÓN
Identity Provider (MIDaaS provider: la operadora de telecomunicaciones)
Relying Party
End User
MID Proxy
Authorization Server
Token Endpoint
UserInfo + Context Endpoint
1. Crear petición de autorización
2. Lanzar petición de autorización
3. Petición no validada y registrada
4a No se da permiso para autenticar al EU
4b Validación negativa de la petición de autorización
UserInfo + Context Endpoint
Token Endpoint
Authorization Server
MID Proxy
End User
Relying Party

Fig. 4

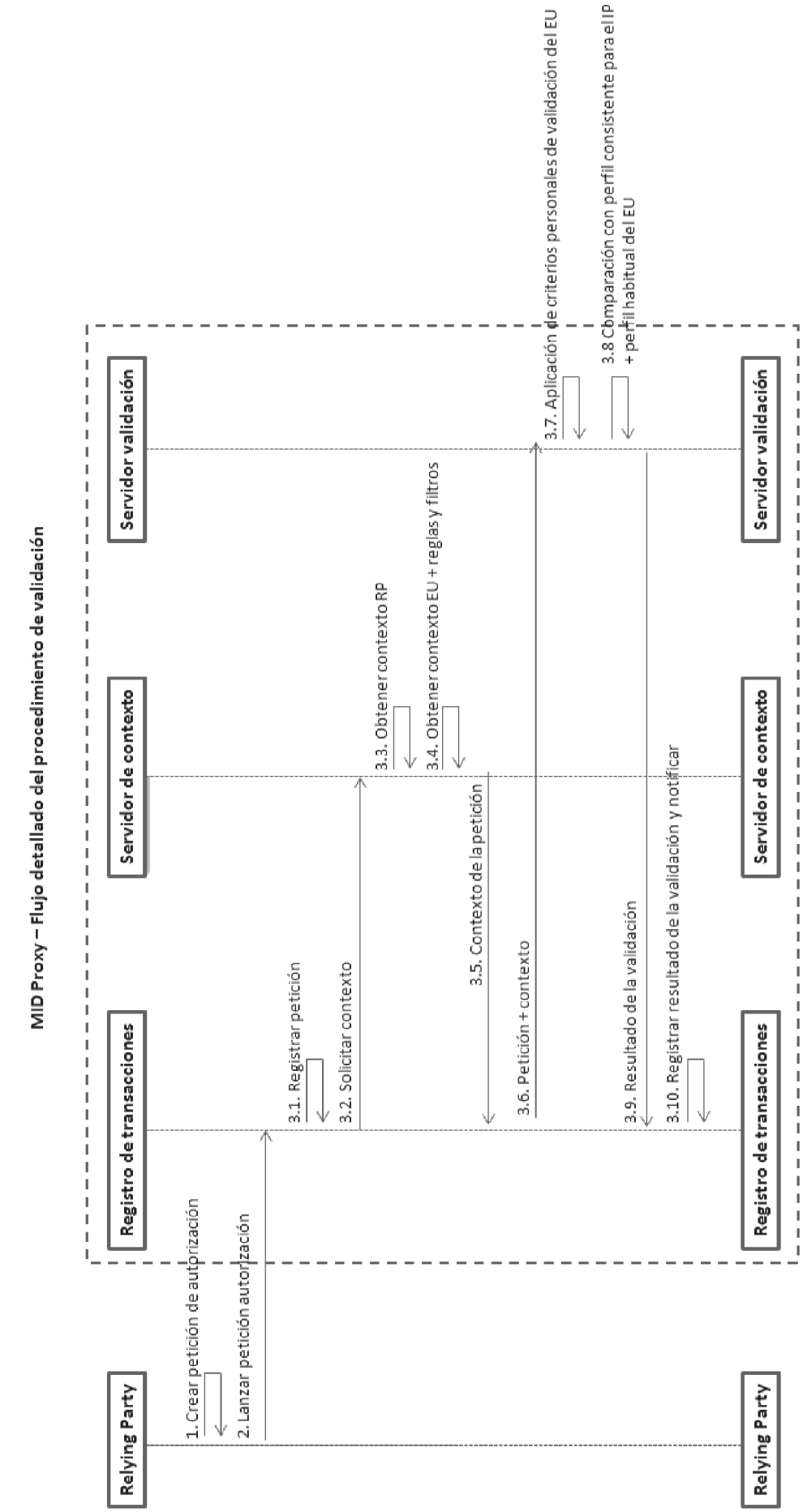
MID Proxy – Flujo detallado del procedimiento de validación
Relying Party
Registro de transacciones
Servidor de contexto
Servidor validación
1. Crear petición de autorización
2. Lanzar petición autorización
3.1. Registrar petición
3.2. Solicitar contexto
3.3. Obtener contexto RP
3.4. Obtener contexto EU + reglas y filtros
3.5. Contexto de la petición
3.6. Petición + contexto
3.7. Aplicación de criterios personales de validación del EU
3.8 Comparación con perfil consistente para el IP + perfil habitual del EU
3.9. Resultado de la validación
3.10. Registrar resultado de la validación y notificar

Fig. 5

Fig. 6

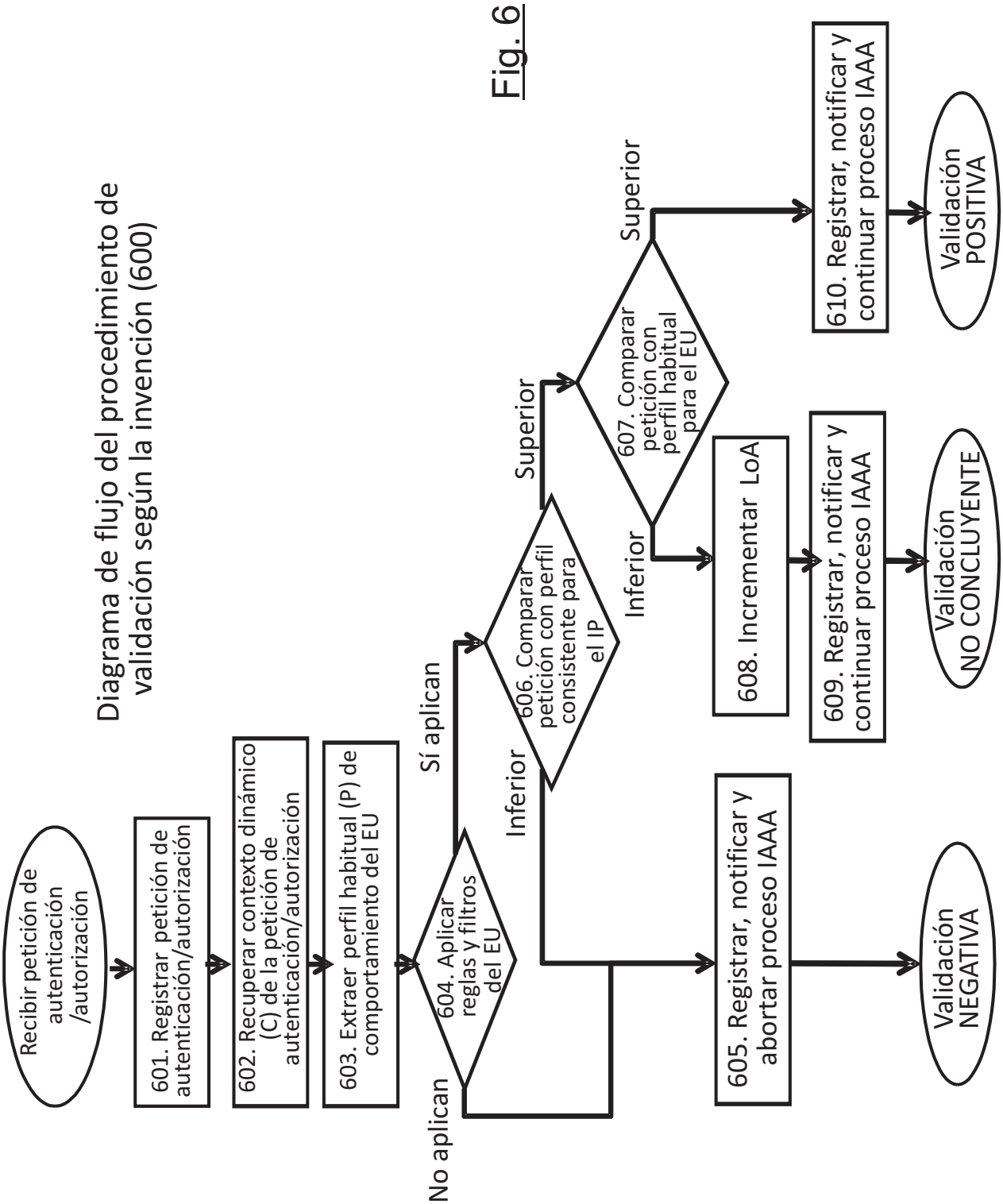
Diagrama de flujo del procedimiento de validación según la invención (600)
Recibir petición de autenticación /autorización
601. Registrar petición de autenticación/autorización
602. Recuperar contexto dinámico (C) de la petición de autenticación/autorización
603. Extraer perfil habitual (P) de comportamiento del EU
604. Aplicar reglas y filtros del EU
Sí aplican
No aplican
606. Comparar petición con perfil consistente para el IP
Superior
Inferior
607. Comparar petición con perfil habitual para el EU
Superior
Inferior
608. Incrementar LoA
605. Registrar, notificar y abortar proceso IAAA
609. Registrar, notificar y continuar proceso IAAA
610. Registrar, notificar y continuar proceso IAAA
Validación NEGATIVA
Validación NO CONCLUYENTE
Validación POSITIVA

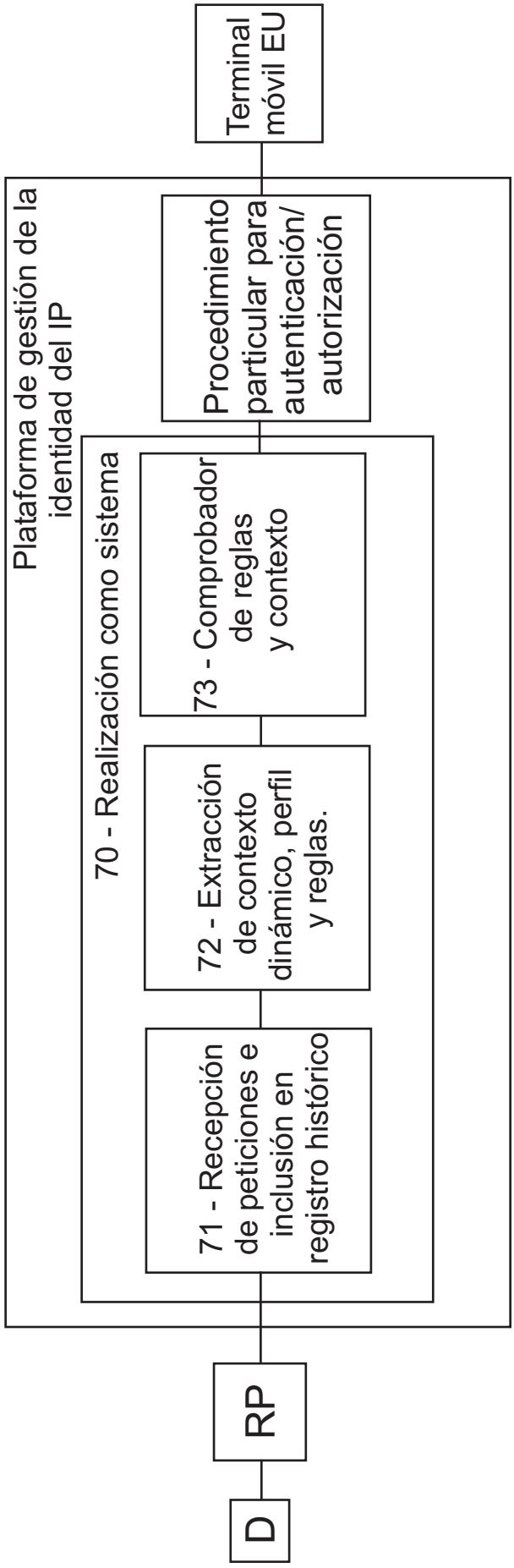
Terminal móvil EU
Plataforma de gestión de la identidad del IP
Procedimiento particular para autenticación/ autorización
70 - Realización como sistema
73 - Comprobador de reglas y contexto
72 - Extracción de contexto dinámico, perfil y reglas.
71 - Recepción de peticiones e inclusión en registro histórico
RP
D

Fig. 7

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201531491

(22) Fecha de presentación de la solicitud: 15.10.2015

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04W12/06*** (2009.01)
H04W12/08 (2009.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	WO 2014176539 A1 (INTERDIGITAL PATENT HOLDINGS) 30.10.2014, figuras 1,2; párrafos [42-54,61,64,65,75-96,123-126,140-147].	1-11
X	US 2015172269 A1 (CHA INHYOK et al.) 18.06.2015, párrafos [32,34,38,45-49,57,64,79,80,84-87,91,95,98,105,107-118,134,138].	1-11

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

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
28.06.2016	B. Pérez García	1/5

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

H04W, H04L

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

INVENES, EPODOC, WPI, INSPEC

Fecha de Realización de la Opinión Escrita: 28.06.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	6-10	**SI**
	Reivindicaciones	1-5,11	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-11	**NO**

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

Base de la Opinión.-

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

1. Documentos considerados.-

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

Documento	Número Publicación o Identificación	Fecha Publicación
D01	WO 2014176539 A1 (INTERDIGITAL PATENT HOLDINGS)	30.10.2014
D02	US 2015172269 A1 (CHA INHYOK et al.)	18.06.2015

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

Se considera D01 el documento del estado de la técnica anterior más cercano al objeto de la solicitud.

Se citan en cursiva las referencias equivalentes a las de la solicitud y que aparecen en D01.

Siguiendo la redacción de la primera reivindicación, D01 describe un procedimiento para la validación de una petición de autenticación/autorización de un usuario *(UE 102)* caracterizado porque comprende:
- recibir, desde un proveedor de servicios *(RP 104)*, una petición de autenticación/autorización de un usuario *(UE 102)* – *párrafo 61*;
- extraer el contexto dinámico de la petición recibida del proveedor de servicios, donde dicho contexto comprende reglas definidas por el usuario para su identidad *(párrafo 50: "El MFAS 106 puede dinámicamente generar las políticas requeridas y ejecutar esas políticas generadas en base a un nivel de seguridad dada. La información recibida por el MFAS para generar las políticas incluye políticas de usuario, políticas del SP, requisitos para acceder a un servicio concreto proporcionado por el SP…"; párrafo 124: "el mapeo del nivel de seguridad puede cambiar con el tiempo, por ej, las capacidades de autenticación del dispositivo pueden cambiar según se habiliten o deshabiliten características, basándose en preferencias cambiantes del usuario");*
- extraer el perfil asociado a dicha identidad, donde dicho perfil contiene información extraída de contextos históricos asociados a peticiones y transacciones pasadas realizadas desde dicha identidad *(párrafo 65: "Cuando se detectan las capacidades de autenticación, una asociación segura entre cada capacidad y cada usuario se mantiene en el SP o en el IdP. Esta asociación permite más tarde establecer un nivel de seguridad que corresponde a un usuario y a un protocolo de autenticación particular que puede ser requerido por un SP específico. Esta asociación de factores de autenticación y de usuarios o de identificadores de UE puede almacenarse en una base de datos de autenticación de usuario, que puede residir en el MFAS 106"; párrafo 79: "la vigencia de cada factor de autenticación es chequeada para determinar si un resultado de autenticación previa puede reutilizarse evitando al usuario repetir el proceso de autenticación")*;
- comprobar el cumplimiento de las reglas incluidas en el contexto por la petición recibida para establecer la validación de dicha petición, y decidir si elevar el nivel de seguridad (LoA) asociado a dicha petición *(párrafo 123:"Una aplicación de banco puede solicitar un nivel de seguridad de autenticación alto, biométrico, para acceder a la cuenta. Si el UE no tiene capacidades biométricas, el IdP puede negociar con el RP. IdP puede ofrecer una autenticación adecuada a las capacidades del dispositivo y entonces la RP puede degradar el servicio que proporciona. En otra realización, IdP puede proporcionar un protocolo para incrementar el nivel de seguridad al nivel deseado")"*;
- enviar al proveedor de servicios (RP) información sobre la validación de la petición de autenticación/autorización y sobre la decisión de elevar el nivel de seguridad (LoA) *(párrafo 96: "el nivel de seguridad obtenido y otra información sobre las autenticaciones realizadas se comunican a la RP")*.

No se han encontrado diferencias entre ambos documentos, y por tanto, se considera que la primera reivindicación no cumple el requisito de novedad según el Art. 6 de la Ley 11/1986.

La segunda reivindicación indica que la petición de autenticación/autorización del usuario es almacenada para permitir su trazabilidad y para actualizar el perfil asociado a la identidad.
Los párrafos 78 y 79 de D01 indican que *los factores de autenticación pueden registrarse y sincronizarse con una entidad de políticas de red. Un registro almacenado puede incluir un código de sesión, una indicación de la autenticación específica llevada a cabo, un número de intentos, el resultado de la autenticación… La validez de cada factor de autenticación se comprueba para determinar si un resultado de autenticación previa puede reutilizarse sin hacer que el usuario repita el proceso de autenticación.*
A la luz de estos párrafos, esta segunda reivindicación carece de novedad.

La tercera reivindicación define que un subconjunto de reglas es definido por el usuario y la cuarta que un subconjunto de reglas es definido por la operadora de comunicaciones.
Como se ha comentado anteriormente, estas características aparecen descritas en el párrafo 50 de D01. Sin novedad.

La reivindicación número cinco añade que si el grado de cumplimiento de las reglas definidas por el usuario es inferior a un primer umbral de confianza, la validación es negativa y se finaliza.
Este paso está definido en el párrafo 91 de D01. Sin novedad.

Las reivindicaciones 6, 7 y 9 definen políticas de acceso según diferentes umbrales de confianza en base a las reglas definidas por el EU y la operadora de telecomunicaciones. Estas reivindicaciones quedan anticipadas por los párrafos 142-145 de D01 y ya que las diferencias que producen son meras alternativas que no contribuyen al resultado técnico de la invención, se considera que no presentan actividad inventiva para un experto en la materia, según el Art. 8 de la LEP.

Las reivindicaciones 8 y 10 enuncian, respectivamente, que se notifica a la RP y al terminal de usuario el nuevo nivel de seguridad.
La reivindicación 8 está reflejada en el párrafo 96 de D01 como se ha citado anteriormente. Respecto a la reivindicación 10, el hecho de comunicarle al terminal de usuario el nuevo nivel de seguridad no se considera que produzca un efecto técnico diferenciador y por tanto, no se considera que tenga actividad inventiva.

La última reivindicación se refiere al sistema que implementa el método anterior y aplicando el mismo razonamiento que para éste, se considera que no tiene novedad a la luz de la descripción realizada en D01.

En resumen, la solicitud presentada no tiene novedad para las reivindicaciones 1-5 y 11 según el Art. 6 y carece de actividad inventiva para las reivindicaciones 6-10 según el Art. 8 de la Ley Española de Patentes.