(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 959 808**

(51) Int. Cl.:

H04L 9/40 (2012.01)
H04L 9/08 (2006.01)
G06F 21/10 (2013.01)
G06F 21/55 (2013.01)
G06F 21/60 (2013.01)
G06F 21/62 (2013.01)
H04L 9/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.02.2017 PCT/US2017/015958**

(87) Fecha y número de publicación internacional: **17.08.2017 WO17139145**

(96) Fecha de presentación y número de la solicitud europea: **01.02.2017 E 17750582 (3)**

(97) Fecha y número de publicación de la concesión europea: **04.10.2023 EP 3414866**

(54) Título: **Control de acceso para datos digitales**

(30) Prioridad:

08.02.2016 US 201615018643

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.02.2024

(73) Titular/es:

MALIKIE INNOVATIONS LIMITED (100.0%)
The Glasshouses GH2, 92 Georges Street Lower
Dun Laoghaire, Dublin A96 VR66, IE

(72) Inventor/es:

CHANDA, RUPEN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Control de acceso para datos digitales

Campo de la descripción

La presente descripción se refiere, en general, al control del acceso a datos y, más en particular, a la provisión de autorización para que dispositivos accedan a datos controlados.

Antecedentes

Los datos pueden almacenarse en muchos tipos de sistemas y dispositivos que permiten que varios dispositivos o usuarios accedan a dichos datos. Los datos con acceso controlado pueden incluir muchos tipos de información como, por ejemplo, documentos, imágenes, datos de vídeo, definiciones de recursos de procesamiento, otros datos, o combinaciones de estos. Los datos que incluyen información sensible pueden protegerse por varias técnicas. Ejemplos de técnicas usadas para proteger datos incluyen Gestión de Derechos Digitales (DRM, por sus siglas en inglés) y Gestión de Derechos de la Información (IRM, por sus siglas en inglés). Estas técnicas con frecuencia incluyen cifrar los datos y exigir el cumplimiento del control de acceso a los datos. En algunas técnicas, el control de acceso se provee por una combinación de nombre de usuario y contraseña que se ingresa para obtener acceso al documento. En algunos ejemplos, dichos datos pueden almacenarse en dispositivos que están disponibles para muchos otros dispositivos como, por ejemplo, datos almacenados en servidores conectados a Internet.

El documento US 2010/005511 describe sistemas y métodos para autorizar una solicitud para acceder a un recurso según un contexto de la solicitud. El método comprende recibir la solicitud de un solicitante, identificar el contexto de la solicitud, y determinar si autorizar la solicitud según el contexto de la solicitud. La solicitud puede incluir información de contexto que describe el contexto de la solicitud e identificar el contexto según al menos en parte la información de contexto de la solicitud.

El documento US2004/111645 describe un método para proveer control de acceso a redes informáticas de registro único. Un verificador de perfil monitorea la solicitud de un usuario para acceder a cualquier recurso dentro de la red informática. Un generador de perfil añade la información de la solicitud de acceso a un perfil de usuario existente. La solicitud de acceso pasa entonces a través del verificador de parámetro para determinar si la solicitud de acceso viola ciertos parámetros predefinidos. Un gestor de sesión verifica si una solicitud de acceso del usuario podrá basarse en el perfil de usuario. Si la respuesta es sí, el gestor de sesión entonces concede la solicitud de acceso sin acciones adicionales. Si la respuesta es no, el gestor de sesión entonces envía una gravedad que significa cuánto se desvía la solicitud de acceso del patrón de acceso normal, para indicar que el patrón de uso del usuario está fuera del comportamiento normal.

El documento US2007113270A1 describe un recurso de red/ordenador, p. ej., impresora, método de establecimiento de permiso de acceso para, p. ej., servidor, que implica proveer respuesta automática que incluye la concesión de permiso de acceso a la consulta de permiso de aplicación si el modo aprendizaje está activo y consultar a usuarios los permisos de acceso si el modo de aprendizaje no está activo en caso de que se detecte una desviación del comportamiento de referencia.

Breve descripción de los dibujos

Las figuras anexas donde numerales de referencia iguales se refieren a elementos idénticos o funcionalmente similares a lo largo de las vistas separadas, y que, junto con la descripción detallada de más abajo, se incorporan y forman parte de la memoria descriptiva, sirven para ilustrar varias realizaciones y para explicar varios principios y ventajas según la presente descripción, en la cuales:

La Figura 1 ilustra un entorno de acceso a datos, según un ejemplo;

la Figura 2 ilustra una interfaz de configuración de protección de conjunto de datos, según un ejemplo;

la Figura 3 ilustra un proceso de evaluación de solicitud de acceso, según un ejemplo;

la Figura 4 ilustra un proceso de gestión de notificaciones, según un ejemplo;

la Figura 5 ilustra una visualización de contexto de notificación, según un ejemplo; y

la Figura 6 es un diagrama de bloques de un dispositivo electrónico y componentes asociados en el cual pueden implementarse los sistemas y métodos descritos en la presente memoria.

Descripción detallada

Por consiguiente, se provee un método según se detalla en la reivindicación 1 y un dispositivo según se detalla en la reivindicación 4, y un medio de almacenamiento legible por ordenador detallado en la reivindicación 6. Características ventajosas se proveen en las reivindicaciones dependientes.

Según lo requerido, realizaciones detalladas se describen en la presente memoria; sin embargo, se comprenderá que las realizaciones descritas son meramente ejemplos y que los sistemas y métodos descritos más abajo pueden realizarse en varias formas. Por lo tanto, detalles estructurales y funcionales específicos descritos en la presente memoria no se interpretarán como restrictivos, sino meramente como una base para las reivindicaciones y como una base representativa para enseñar a una persona con experiencia en la técnica a emplear, de forma variada, el presente objeto en prácticamente cualquier estructura y función detalladas de manera apropiada. Además, los términos y frases usadas en la presente memoria no pretenden ser restrictivos, sino más bien, proveer una descripción comprensible de los conceptos.

Los términos "un", "una" o "uno", según su uso en la presente memoria, se definen como uno o más de uno. El término "múltiples", según su uso en la presente memoria, se define como dos o más de dos. El término "otro/a", según su uso en la presente memoria, se define como al menos un/a segundo/a o más. Los términos "que incluye(n)" y "que tiene(n)", según su uso en la presente memoria, se definen como que comprende(n) (a saber, lenguaje abierto). El término "acoplado/a(s)", según su uso en la presente memoria, se define como conectado/a(s), aunque no necesariamente de forma directa, y no necesariamente de manera mecánica. El término "configurado/a(s) para" describe hardware, software o una combinación de hardware y software que se adapta para, se configura, se dispone, se construye, se compone, está diseñada o que tiene cualquier combinación de estas características para llevar a cabo una función dada. El término "adaptado/a(s) para" describe hardware, software o una combinación de hardware y software que tiene capacidad para, puede alojar, llevar a cabo, o que es adecuada para llevar a cabo una función dada.

Los sistemas y métodos descritos más abajo funcionan para proveer autorización para acceder a datos según el contexto del dispositivo que solicita acceso a los datos. En varios ejemplos, un contexto de un dispositivo que solicita acceso puede incluir cualquier caracterización del dispositivo o cualquier condición asociada al dispositivo. Por ejemplo, un contexto del dispositivo puede incluir, sin limitación, uno o más de los siguientes: una fecha u hora de la solicitud de acceso, una ubicación geográfica del dispositivo al momento de realizar la solicitud de acceso, una dirección de Protocolo de Internet (IP, por sus siglas en inglés) del dispositivo que realiza la solicitud de acceso, datos que describen software que se está usando por el dispositivo que realiza la solicitud de acceso, un identificador de dispositivo (ID, por su siglas en inglés) del dispositivo que realiza la solicitud de acceso, cualquier otra descripción de contexto, o combinaciones de estos.

Los datos pueden estar disponibles para uno o más dispositivos solicitantes por cualquier técnica adecuada. Por ejemplo, un dato puede entregarse al dispositivo solicitante mediante cualquier técnica adecuada como, por ejemplo, mediante comunicaciones electrónicas. En un ejemplo, los datos pueden asegurarse por cualquier técnica adecuada de modo que se requiere que la autorización externa lleve a cabo una o más funciones con los datos. Funciones para las cuales la autorización puede especificarse que se requiere incluyen, por ejemplo, ver los datos, acceder a los datos mediante cualquier técnica adecuada, usar los datos, modificar los datos, enviar los datos a cualquier otro dispositivo o dispositivos, de otra manera acceder a o usar parte de o todos los datos, o cualquier otra operación o proceso. Los datos pueden estar disponibles para el dispositivo solicitante por cualquier técnica adecuada como, por ejemplo, al estar almacenados en el dispositivo solicitante, al acceder a ellos por el dispositivo solicitante mediante comunicaciones con un dispositivo de almacenamiento, por cualquier otra técnica de recuperación adecuada, o combinaciones de estos.

El acceso a datos protegidos puede controlarse por cualquier técnica adecuada. Ejemplos de técnicas de control de acceso para datos protegidos incluyen Gestión de Derechos Digitales (DRM) y Gestión de Derechos de la Información (IRM). En un ejemplo, las técnicas de Gestión de Derechos Digitales (DRM) pueden aplicarse para limitar el acceso a los datos y limitar los usos permitidos de los datos. En un ejemplo, el acceso a datos con acceso controlado por técnicas DRM puede incluir solicitar una clave de descifrado u otro testigo de autorización de un servidor remoto que supervisa el control de acceso de los datos. La solicitud de dicha calve de descifrado u otro testigo de autorización es un ejemplo de una solicitud de acceso llevada a cabo por un dispositivo solicitante. Ejemplos de solicitudes de acceso incluyen un dispositivo solicitante que envía una solicitud de una clave DRM de un servidor de clave DRM con el fin de acceder a datos protegidos por técnicas DRM. En algunos ejemplos, programas de aplicación que pueden acceder a tipos particulares de datos incluyen procesamiento para soportar la solicitud de una clave DRM para acceder a los datos. El servidor de clave DRM puede determinar si una clave DRM se proveerá al dispositivo solicitante. En algunos casos, la clave DRM puede limitar el tipo de usos para los cuales pueden usarse los datos.

Los datos con respecto a los cuales el acceso es controlado o protegido pueden ser cualquier tipo de datos. En un ejemplo, los datos protegidos y con respecto a los cuales el acceso es controlado pueden incluir cualquier contenido, componentes, recursos, datos (p. ej., documentos, archivos, correos electrónicos, mensajes, imágenes, vídeo, medios, o cualquier dato digital), cualquier otro tipo de dato, o combinaciones de estos. En un ejemplo, se dice que los datos que están protegidos o con respecto a los cuales el acceso es controlado se crean cuando un usuario u otro proceso aplica el esquema de protección o control de acceso a los datos a un conjunto particular de datos. En el contexto de la siguiente descripción, la creación de datos protegidos se refiere a la aplicación y configuración de cualquier control de acceso, protecciones de datos, cualquier otro tipo de control, o combinaciones de estos, a cualquier dato independientemente de si los datos ya existen, se están creando, se modificarán por procesamiento futuro, son cualquier tipo de dato, o combinaciones de estos.

En algunos ejemplos, las solicitudes asociadas a datos particulares se registran con el fin de soportar la determinación

de un patrón de acceso. Las solicitudes que pueden registrarse incluyen, pero sin limitación a, solicitudes de acceso a todos o parte de datos particulares, solicitudes de acceso a todos o parte de datos particulares para uno o más usos particulares, solicitudes de acceso a todos o parte de datos particulares para cualquier uso o para un uso o usos particulares por un dispositivo solicitante particular. Los patrones de acceso en varios ejemplos incluyen cualquier caracterización del acceso a datos protegidos por técnicas DRM. Los patrones de acceso en varios ejemplos pueden incluir, sin limitación, características como, por ejemplo, cualquiera de las siguientes: ubicaciones desde las cuales los dispositivos solicitantes solicitan acceso, la cantidad de tiempo durante el cual el dispositivo solicitante accede a los datos, las operaciones que se solicita que se lleven a cabo en los datos, la frecuencia con la cual las operaciones particulares se solicita que se lleven a cabo, la cantidad de datos sobre los cuales se llevará a cabo una operación, cualquier otra caracterización o caracterizaciones, o combinaciones de estas. Los patrones de acceso pueden también incluir caracterizaciones de circunstancias en las cuales los dispositivos solicitantes solicitan el acceso, como si el dispositivo solicitante se está comunicando en una conexión Wi-Fi®, conexión de datos celular, conexión de datos cableada, u otros tipos de conexiones de datos. Los patrones de acceso pueden también definir cómo otros dispositivos solicitan acceso como, por ejemplo, si muchos dispositivos solicitan acceso a datos particulares al mismo tiempo, en momentos similares, dentro de intervalos de tiempo particulares uno con respecto al otro, u observaciones similares. Los patrones de acceso pueden definirse o crearse por cualquier técnica adecuada. Por ejemplo, un patrón de acceso puede definirse según un historial acumulado de solicitudes de acceso para datos o grupos de datos particulares. En ejemplos adicionales, los patrones de acceso pueden basarse en, por ejemplo, rangos especificados de contextos para dispositivos solicitantes, contextos observados de dispositivos solicitantes para datos o un grupo de datos particulares, según cualquier técnica, o según cualquier combinación de estos. En general, un patrón de acceso puede asociarse a un conjunto de datos, con un grupo de datos con el grupo definido según cualquier técnica adecuada, o con combinaciones de estos.

En un ejemplo, las solicitudes de acceso a datos particulares pueden hacer que una notificación de la solicitud de acceso se envíe a un dispositivo de autorización especificado. En un ejemplo, un dispositivo de autorización se usa por una persona en quien se confía para que controle y autorice el acceso a datos particulares. En varios ejemplos, cada conjunto de datos, o un grupo de datos, puede asociarse a un dispositivo de autorización particular al cual se envían notificaciones de solicitudes de acceso. En un ejemplo, las notificaciones pueden enviarse a un dispositivo de autorización según comparaciones del contexto del dispositivo solicitante que envía la solicitud de acceso con patrones de acceso determinados asociados a los datos.

En algunos ejemplos, la autorización para acceder a datos puede basarse en un proceso automatizado que evalúa el contexto del dispositivo solicitante con criterios para determinar si una solicitud de acceso es probablemente legítima y puede concederse, o si el contexto del dispositivo solicitante indica que la solicitud de acceso puede ser sospechosa y, por lo tanto, rechazada. Procesos automatizados para determinar si una solicitud debe concederse o rechazarse pueden incluir cualquier tipo de procesamiento de evaluación, incluidos, por ejemplo, inteligencia artificial, árboles de decisión, otras técnicas, o combinaciones de estos. En algunos ejemplos, un proceso automatizado puede determinar si el contexto de un dispositivo solicitante se encuentra dentro de los criterios para permitir el acceso a los datos dentro de datos particulares, y si dicho proceso automatizado no logra determinar que el acceso debe concederse, una notificación se envía a un dispositivo de autorización para permitir a un usuario de dicho dispositivo determinar si el acceso debe concederse o denegarse.

En un ejemplo, la configuración del acceso DRM para datos particulares puede incluir una especificación del tipo de procesamiento de autorización que se aplicará. Por ejemplo, una persona que crea datos protegidos que se protegen por, por ejemplo, técnicas DRM, puede especificar que todas las autorizaciones para dichos datos se provean según una respuesta a una notificación enviada a un dispositivo de autorización. En otro ejemplo, el creador de dichos datos protegidos puede especificar condiciones para las cuales se permitirá la autorización automatizada como, por ejemplo, en respuesta a solicitudes de acceso en cierta área geográfica o dentro de un rango de dirección de Protocolo de Internet especificado, y solicitudes de acceso que no satisfacen dichas condiciones especificadas solo se concederán según una respuesta a una notificación a un dispositivo de autorización. En incluso un ejemplo adicional, el creador de datos protegidos puede especificar que todas las solicitudes de acceso se gestionen por un proceso automatizado que lleva a cabo una evaluación automatizada del contexto del dispositivo solicitante. En un ejemplo, la selección entre estos diferentes tipos de procesamiento de autorización puede basarse en un juicio de sensibilidad de los datos y el impacto que podría tener la propagación no autorizada de dichos datos. En este contexto, la creación de datos protegidos se refiere a la configuración de la protección, control de acceso, otro control, o combinaciones de estos, a datos independientemente de si dichos datos ya existen, se están creando, son datos que se refieren a otros datos que se crearán o modificarán en el futuro, son cualquier tipo de datos, o combinaciones de estos.

En algunos ejemplos, las decisiones de permitir o denegar solicitudes de acceso pueden además basarse en políticas de acceso a datos. Por ejemplo, una compañía puede tener una política de que los empleados no accederán a ciertos datos desde países particulares. Las solicitudes de acceso desde dichos países se denegarán.

La Figura 1 ilustra un entorno 100 de acceso a datos, según un ejemplo. El entorno 100 de acceso a datos representa un dispositivo 130 solicitante que puede usar datos protegidos. Una red 160 en este ejemplo ilustrado se usa para soportar comunicaciones de datos entre múltiples dispositivos como, por ejemplo, el dispositivo 130 solicitante ilustrado y un gestor 102 de clave DRM. La red 160 también puede soportar comunicaciones de datos entre otros dispositivos como, por ejemplo, se describe más abajo.

El dispositivo 130 solicitante en este ejemplo accede a datos protegidos por técnicas DRM mediante el envío de solicitudes de acceso a un gestor 102 de clave DRM. El gestor 102 de clave DRM en este ejemplo puede condicionar la concesión de acceso a datos protegidos según autorizaciones provistas por un módulo 104 de análisis de seguridad de usuario. Si el módulo 104 de análisis de seguridad de usuario permite al dispositivo solicitante llevar a cabo el uso solicitado de los datos, el gestor 102 de clave DRM recupera un testigo de autorización como, por ejemplo, la clave DRM, de un almacenamiento 110 de claves para los datos y envía dicho testigo de autorización al dispositivo solicitante. En un ejemplo, el módulo 104 de análisis de seguridad de usuario incluye un procesador programable que se configura para ejecutar programas para implementar un procesador de contexto que funciona según los ejemplos descritos en la presente memoria. El módulo 104 de análisis de seguridad de usuario además incluye una interfaz de datos que recibe solicitudes de acceso de dispositivos solicitantes para acceder a un dato solicitado. En un ejemplo, esta interfaz de datos se comunica con el gestor 102 de clave DRM. En ejemplos adicionales, la interfaz de datos del módulo 104 de análisis de seguridad de usuario puede comunicarse con otros componentes como, por ejemplo, con el propio dispositivo solicitante ya sea de manera directa o a través de cualquier otro componente intermedio.

El dispositivo 130 solicitante incluye un almacenamiento 134 que se muestra que contiene datos 136 protegidos. En varios ejemplos, el almacenamiento 134 puede almacenar una cantidad de conjuntos de datos, algunos de los datos estando protegidos, algunos no estando protegidos, o combinaciones de estos. En algunos ejemplos, otros datos 154 protegidos pueden almacenarse en una ubicación remota como, por ejemplo, en un almacenamiento 152 en la nube que es accesible para el dispositivo 130 solicitante mediante cualquier técnica de comunicaciones electrónicas adecuada.

El dispositivo 130 solicitante en un ejemplo incluye varios programas de aplicación u otras instalaciones para usar datos protegidos como, por ejemplo, los datos 136. Dichos programas de aplicación u otras instalaciones pueden funcionar con una interfaz 132 DRM en un ejemplo con el fin de comunicarse con un gestor 102 de clave DRM para recibir testigos de acceso como, por ejemplo, una clave DRM, usados para permitir el acceso a los datos 136 protegidos. En general, un dispositivo 130 solicitante puede usar cualquier técnica adecuada para acceder a datos protegidos.

El gestor 102 de clave DRM en este ejemplo recibe solicitudes para acceder a datos protegidos desde dispositivos remotos como, por ejemplo, el dispositivo 130 solicitante ilustrado. En general, puede haber una gran cantidad de dispositivos solicitantes que se comunican con el gestor 102 de clave DRM para solicitar acceso a varios datos protegidos. Algunas de las solicitudes de acceso recibidas por el gestor 102 de clave DRM pueden incluir información sobre un contexto del dispositivo solicitante. El contexto del dispositivo solicitante puede incluir cualquier característica como, por ejemplo, aquellas descritas más arriba, del dispositivo solicitante. En un ejemplo, el contexto recibido de un dispositivo solicitante incluye la ubicación geográfica del dispositivo solicitante que presenta la solicitud de acceso.

El gestor 102 de clave DRM en un ejemplo se configura para enviar solicitudes de acceso para al menos algunos datos protegidos a un módulo 104 de análisis de seguridad de usuario. Dichas solicitudes de acceso incluyen información de contexto sobre el dispositivo solicitante que envía la solicitud de acceso. El módulo 104 de análisis de seguridad de usuario en un ejemplo registra solicitudes de acceso recibidas junto con el contexto del dispositivo solicitante. En un ejemplo, el módulo 104 de análisis de seguridad de usuario determina datos 112 de patrón de acceso según el análisis de las múltiples solicitudes de acceso recibidas y los contextos de los dispositivos solicitantes que envían dichas solicitudes. En un ejemplo, características, o contextos, típicas de dispositivos solicitantes pueden determinarse mediante análisis de una cantidad de solicitudes de acceso recibidas. Una solicitud de acceso recibida posteriormente puede entonces compararse en algunos ejemplos con las características típicas definidas en los datos de patrón de acceso para determinar si la solicitud de acceso posteriormente recibida es coherente con, o anómala con respecto a, las características típicas que se han observado para el acceso a los datos protegidos para los cuales se recibe la solicitud de acceso.

El módulo 104 de análisis de seguridad de usuario además contiene reglas 114 de acceso que definen el tipo de decisión que se tomará cuando se conceda el acceso a los datos protegidos. En un ejemplo, cuando los datos protegidos se configuran con, p. ej., controles DRM sobre su uso, un usuario que configura la protección a aplicarse a los datos puede definir varias reglas 114 de acceso. Ejemplos de reglas 114 de acceso se describen en mayor detalle más abajo.

En varios ejemplos, las reglas 114 de acceso para datos protegidos o un grupo de datos protegidos particulares pueden tener cualquiera de varios modos de decisión especificados para cada tipo de uso de cada componente de datos protegidos. Un tipo de modo de decisión de acceso incluye enviar una notificación de la solicitud de acceso a un dispositivo de autorización especificado de modo que un usuario de dicho dispositivo de autorización puede evaluar la solicitud de acceso y determinar si la solicitud de acceso se permite o deniega. Otro tipo de modo de decisión de acceso es una decisión de acceso automatizada en donde el contexto de un dispositivo que envía una solicitud de acceso se compara con varias definiciones de contexto para determinar, de forma automática, si el acceso solicitado se concederá o denegará. En varios ejemplos, dichas decisiones de acceso automatizadas pueden basarse en cualquier técnica de evaluación como, por ejemplo, comparación con definiciones de contexto definidas, evaluación por un proceso de inteligencia artificial que usa cualquier técnica adecuada para evaluar el contexto del dispositivo solicitante que presenta la solicitud de acceso según solicitudes de acceso previamente recibidas, cualquier otra técnica, o combinaciones de estas. En algunos ejemplos, las reglas de acceso pueden especificar que no se requiere una decisión de acceder a los datos.

El módulo 104 de análisis de seguridad de usuario en un ejemplo puede enviar solicitudes de decisión a un módulo 106 de decisión. El módulo 106 de decisión en un ejemplo lleva a cabo el procesamiento para soportar la decisión especificada sobre si permitir o denegar una solicitud de acceso solicitada. En un ejemplo, la solicitud de decisión enviada por el módulo 104 de análisis de seguridad de usuario puede especificar si una decisión se basará en una determinación automatizada o se basará en una respuesta a una notificación provista a un dispositivo de autorización. En ejemplos adicionales, otros tipos de decisiones pueden soportarse por el módulo 106 de decisión.

En el caso de una decisión automatizada, el módulo 106 de decisión funciona con un procesador 116 de decisiones autónomo. El procesador 116 de decisiones autónomo en un ejemplo implementa varios procesamientos automatizados para evaluar si la solicitud de acceso recibida se permitirá o denegará. El procesador 116 de decisiones autónomo puede acceder a datos 112 de patrón determinados por el módulo 104 de análisis de seguridad de usuario para soportar la decisión de permitir o denegar la solicitud de acceso. Detalles de las decisiones automáticas tomadas por el procesador 116 de decisiones autónomo se describen en detalle más abajo.

En el caso de una decisión que se basará en una notificación enviada a un dispositivo de autorización, el módulo 106 de decisión funciona con un gestor 118 de notificaciones. El gestor 118 de notificaciones en un ejemplo envía notificaciones a un dispositivo 120 de autorización. En un ejemplo, el dispositivo 120 de autorización particular al cual enviar las solicitudes de acceso para datos particulares puede definirse en las reglas 114 de acceso. El gestor 118 de notificaciones en dicho caso determinará a qué dispositivo 120 de autorización enviar la notificación según el acceso a las reglas 114 de acceso en el módulo 104 de análisis de seguridad de usuario. En ejemplos adicionales, el dispositivo 120 de autorización puede especificarse por cualquier técnica adecuada como, por ejemplo, el envío de todas las notificaciones para tipos particulares de datos a un dispositivo 120 de autorización especificado.

La notificación en varios ejemplos incluye información que describe el contexto del dispositivo 130 solicitante que presenta la solicitud de acceso. Un usuario del dispositivo 120 de autorización puede entonces revisar la descripción del contexto del dispositivo 130 solicitante y determinar si la solicitud se permitirá o denegará. En un ejemplo, el dispositivo 120 de autorización envía una respuesta al gestor 118 de notificaciones que indica si permitir o denegar la solicitud de acceso recibida. En un ejemplo, el gestor 118 de notificaciones se comunica con el dispositivo 120 de autorización mediante la red 150. En ejemplos adicionales, las comunicaciones entre el gestor 118 de notificaciones y el dispositivo 120 de autorización pueden usar cualquier técnica de comunicaciones adecuada o combinaciones de técnicas de comunicaciones.

El gestor 106 de decisión recibe una indicación del procesador 116 de decisiones autónomo o del gestor 118 de notificaciones para permitir o denegar una solicitud de acceso particular. El gestor 106 de decisión en un ejemplo devuelve al módulo 104 de análisis de seguridad de usuario la indicación de permitir o denegar la solicitud de acceso. El módulo 104 de análisis de seguridad de usuario en algunos ejemplos puede incluir la decisión recibida en los datos de patrón de acceso como una base adicional de determinación de contextos que se asocian a solicitudes de acceso permisibles o a solicitudes de acceso que son sospechosas y pueden requerir mayor procesamiento de decisión. En un ejemplo, los historiales de permiso o rechazo de solicitudes de acceso pueden usarse por el procesador 116 de decisiones autónomo como una base adicional para la determinación automática de permitir o rechazar el acceso. Además, historiales de contextos de dispositivos solicitantes para los cuales se han permitido solicitudes de acceso por el módulo 106 de decisión pueden ser una base en determinaciones futuras de qué tipo de determinación de acceso se solicitará del módulo 106 de decisión.

La Figura 2 ilustra una interfaz 200 de configuración de protección de conjunto de datos, según un ejemplo. La interfaz 200 de configuración de protección de conjunto de datos es un ejemplo de una interfaz de usuario que permite a un usuario configurar las protecciones DRM que se aplicarán a los datos. En un ejemplo, la información provista a través de la interfaz 200 de configuración de protección de conjunto de datos se almacena en las reglas 114 de acceso descritas más arriba.

La interfaz 200 de configuración de protección de conjunto de datos incluye una fila 202 de especificación de datos que tiene una etiqueta "DATOS" y una caja 210 de identidad de datos que permite la especificación de los datos para los cuales se está configurando la protección. La caja 210 de identidad de datos en este ejemplo representa "FILA A" y es una representación de una fila de datos que contiene los datos cuyos datos se protegerán. En ejemplos adicionales, puede usarse cualquier identificación adecuada de los datos.

La interfaz 200 de configuración de protección de conjunto de datos incluye una línea 204 "NOTIFICAR SIEMPRE". La línea 204 "NOTIFICAR SIEMPRE" tiene dos cajas de selección, una caja 212 "SÍ" y una caja 214 "NO". En un ejemplo, estas dos cajas de selección son mutuamente excluyentes, de modo que la selección de la caja 212 "SÍ" hace que la caja 214 "NO" se deseleccione, y viceversa. La selección de la caja 212 "SÍ" en este ejemplo configura las reglas de acceso para los datos especificados para hacer que una notificación se envíe a un dispositivo 120 de autorización para todas las solicitudes de acceso para datos dentro de los datos especificados. En algunos ejemplos, este nivel de decisión puede desearse para información muy sensible. En algunos ejemplos, cuando se selecciona la caja 214 "NO", el módulo 104 de análisis de seguridad de usuario determina si el contexto del dispositivo solicitante que envía la solicitud de acceso se encuentra dentro del rango aceptable. Si se determina que el contexto se encuentra dentro de un rango aceptable cuando se selecciona la caja 214 "NO", la solicitud de acceso se permite sin notificar al dispositivo 120 de autorización y puede basarse en otras entradas de módulos de decisión o basarse en otras reglas

114 de acceso definidas.

La interfaz 200 de configuración de protección de conjunto de datos tiene una línea 206 "AUTORIZACIÓN" con una caja 220 "NOTIFICAR" y una caja 222 "AUTOMÁTICA". En un ejemplo, la selección de la caja 222 "NOTIFICAR" cuando la línea 204 "NOTIFICAR SIEMPRE" tiene la caja 214 "NO" seleccionada hace que el módulo 104 de análisis de seguridad de usuario determine si el contexto del dispositivo solicitante que envía la solicitud de acceso no se encuentra dentro de los rangos aceptables antes de enviar una notificación al dispositivo autorizante. Si se selecciona la caja 222 "AUTOMÁTICA", el módulo 106 de decisión basa su decisión en el procesamiento dentro del procesador 116 de decisiones autónomo.

La interfaz 200 de configuración de protección de conjunto de datos tiene una línea 208 "PROXY DE AUTORIZACIÓN". La línea 208 "PROXY DE AUTORIZACIÓN" tiene una caja 230 de entrada de identificador de dispositivo de autorización que permite una especificación de un identificador de un dispositivo 120 de autorización al cual se enviarán las notificaciones. El ejemplo ilustrado representa un identificador de "AUTO" dentro de la caja 230 de identificador de dispositivo de autorización para indicar que las notificaciones deben enviarse a un dispositivo asociado a la persona que configura la protección del conjunto de datos. En general, cualquier dispositivo puede establecerse como el dispositivo, 120, de autorización y en algunos ejemplos múltiples dispositivos pueden especificarse para recibir, todos, las notificaciones de solicitudes de acceso.

La Figura 3 ilustra un proceso 300 de evaluación de solicitud de acceso, según un ejemplo. El proceso 300 de evaluación de solicitud de acceso es un ejemplo de procesamiento llevado a cabo por el módulo 104 de análisis de seguridad de usuario descrito más arriba.

El proceso 300 de evaluación de solicitud de acceso recibe, en 302, una solicitud de acceso de un dispositivo solicitante para acceder a datos. Esta solicitud en un ejemplo incluye una indicación del contexto del dispositivo solicitante. Como se describe más arriba, el contexto del dispositivo solicitante puede ser cualquier contexto adecuado, incluida, por ejemplo, una ubicación geográfica del dispositivo solicitante. En un ejemplo, la determinación de un contexto del dispositivo solicitante incluye extraer datos de contexto de la solicitud de acceso o de otras comunicaciones con el dispositivo solicitante. En algunos ejemplos, información de contexto adicional puede determinarse según información de otras fuentes como, por ejemplo, información de ubicación geográfica para el dispositivo solicitante obtenida de cualquier fuente.

En general, el acceso a datos puede especificar una solicitud de acceder a todos los datos o solo a una porción de los datos. La solicitud de acceder a los datos puede también especificar un tipo particular de acceso como, por ejemplo, acceder para solo ver los datos, acceder para modificar los datos, acceder para reenviar los datos a otros dispositivos, cualquier otro tipo de uso, o combinaciones de estos.

En un ejemplo, el proceso 300 de evaluación de solicitud de acceso determina, en 304, si las reglas de acceso para los datos requieren que un dispositivo 120 de autorización sea notificado siempre de las solicitudes de acceso. En un ejemplo, esta configuración se establece mediante la interfaz 200 de configuración de protección de conjunto de datos descrita más arriba. Si se proveen las notificaciones, la notificación se provee, en 314, y el procesamiento continúa como se describe más abajo.

Si las notificaciones no siempre se proveen, el proceso 300 de evaluación de solicitud de acceso en un ejemplo almacena, en 306, el contexto del dispositivo solicitante y además determina o refina un patrón de acceso para los datos para los cuales se está solicitando acceso. En un ejemplo, los patrones de acceso se determinan observando características que con frecuencia están presentes en los contextos de dispositivos solicitantes que solicitan acceso a los datos para los cuales se recibe la solicitud de acceso. En algunos ejemplos, el patrón de acceso puede registrar contextos de dispositivos solicitantes que han enviado solicitudes de acceso que se han permitido por el módulo 106 de decisión. En algunos ejemplos, un patrón de acceso para nuevos datos se determina según varias solicitudes de acceso inicial que se procesan por el módulo 106 de decisión. En un ejemplo, la determinación de un patrón de acceso puede incluir determinar el patrón de acceso según características de múltiples solicitudes de acceso recibidas para los datos solicitados. La determinación del patrón de acceso también puede basarse en respuestas de autorización recibidas en respuesta a las múltiples solicitudes de decisiones. Por ejemplo, si se toman decisiones para permitir solicitudes de acceso previamente recibidas con características de contexto, un patrón de acceso puede indicar que las solicitudes de acceso de dispositivos solicitantes con contextos similares se adaptan al patrón de acceso y no son sospechosas, de modo que deben permitirse.

El proceso 300 de evaluación de solicitud de acceso continúa determinando, en 308, si el contexto actual se desvía del patrón de acceso determinado. Según se describe más arriba, un patrón de acceso se determina en algunos ejemplos según los contextos de dispositivos solicitantes que han enviado solicitudes de acceso previas para los datos o datos relacionados. Si se determina que el contexto del dispositivo solicitante que ha enviado la solicitud de acceso no se desvía del patrón de acceso identificado en varias solicitudes de acceso previas, el acceso solicitado se autoriza, en 324.

Si se determina que el contexto del dispositivo solicitante que ha enviado la solicitud de acceso se desvía del patrón de acceso, se toma una determinación sobre si la notificación se enviará a un dispositivo 120 de autorización. Si una

notificación no se envía al dispositivo 120 de autorización, una determinación automática de si aprobar o rechazar la solicitud de acceso se lleva a cabo, en 312. Dicha determinación automática puede determinarse por cualquier técnica adecuada como, por ejemplo, mediante aplicación de reglas de decisión firme, reglas de decisión de lógica difusa, técnicas de inteligencia artificial, cualquier otra técnica, o combinaciones de estas. En general, esta determinación automática puede basarse en cualquier factor o factores adecuados, incluidos, entre otros, un contexto presente del dispositivo solicitante, uno o más patrones de solicitudes de acceso por el dispositivo solicitante, uno o más patrones de solicitudes de acceso por un número de dispositivos solicitantes con características contextuales comunes, uno o más patrones de solicitudes de acceso por todos los dispositivos solicitantes, según cualquier información, o según combinaciones de estos.

La determinación automática llevada a cabo, en 312, también puede determinar conceder solamente un subconjunto de los permisos que se han solicitado en la solicitud de acceso recibida. Por ejemplo, un dispositivo solicitante puede enviar una solicitud de acceso para el acceso total a un conjunto de datos. La determinación automática puede decidir, según cualquier contexto adecuado del dispositivo solicitante, conceder acceso de solo lectura al dispositivo solicitante. En otro ejemplo, un dispositivo solicitante puede enviar una solicitud de acceso para imprimir diez (10) páginas de un documento. Según varios criterios como, por ejemplo, un historial de impresión de dicho dispositivo solicitante particular, el proceso automatizado puede determinar solo autorizar el permiso para imprimir 8 páginas. En general, una determinación de permitir un subconjunto de permisos solicitados en una solicitud de autorización puede basarse en cualquier factor o factores adecuados, incluidos, entre otros, factor o factores enumerados más arriba según los cuales se lleva a cabo una determinación automática.

Si se determina que una notificación se enviará a un dispositivo de autorización, ya sea según una configuración de notificar siempre determinada en 304 o una determinación de que la notificación se requiere en 310, la notificación se envía al dispositivo de autenticación, en 314. Esta notificación puede proveer información con respecto al contexto del dispositivo solicitante como, por ejemplo, se presenta en un ejemplo descrito más abajo.

Después de que la notificación se haya enviado, se recibe una respuesta de autorización, en 316. En algunos ejemplos, la no recepción de una respuesta se interpreta como una respuesta de rechazar el acceso. La autorización determinada ya sea según la respuesta de autorización recibida del dispositivo 120 de autenticación o según la determinación automática se determina como positiva o negativa, en 320. Si se determina que la autorización es positiva, en 320, el acceso solicitado en un ejemplo se autoriza y permite. En ejemplos adicionales, según se describe más arriba, la autorización puede especificar que solo un subconjunto de los permisos solicitados se autorice para el dispositivo solicitante, donde el subconjunto es menor que el conjunto total de permisos solicitados. En el caso de una autorización que autoriza solo un subconjunto de los permisos solicitados, el acceso que usa solo el subconjunto de permisos se autoriza, en 324. Si se determina que la autorización no es positiva, en 320, el acceso solicitado se rechaza. El proceso 300 de evaluación de solicitud de acceso entonces finaliza.

La Figura 4 ilustra un proceso 400 de gestión de notificaciones, según un ejemplo. El proceso 400 de gestión de notificaciones en un ejemplo se lleva a cabo por un dispositivo 120 de autorización tras recibir una notificación del gestor 118 de notificaciones.

El proceso 400 de gestión de notificaciones recibe, en 402, una notificación de una solicitud de acceso a datos por un dispositivo solicitante. La notificación contiene indicaciones del contexto del dispositivo solicitante y una indicación del conjunto de datos cuyo acceso se solicita, y puede incluir una indicación del tipo de acceso a los datos que se está solicitando, incluidos los tipos de usos para los cuales se accederá a los datos.

El proceso 400 de gestión de notificaciones presenta, en 404, el contexto del dispositivo solicitante al usuario. Una presentación a modo de ejemplo de un contexto se describe en mayor detalle más abajo.

El proceso 400 de gestión de notificaciones recibe, en 406, una respuesta de autorización de un usuario del dispositivo. La respuesta de autorización puede ser una entrada "PERMITIR" o "RECHAZAR" recibida de un usuario.

El proceso 400 de gestión de notificaciones envía, en 408, una indicación de la respuesta de autorización. En un ejemplo, la indicación puede enviarse otra vez al gestor 118 de notificaciones que ha enviado la notificación. En ejemplos adicionales, la notificación puede enviarse a cualquier destino o destinos adecuados como, por ejemplo, directamente al módulo 104 de análisis de seguridad de usuario, directamente al gestor 102 de clave DRM, a cualquier destino adecuado, o a combinaciones de estos. El proceso 400 de gestión de notificaciones entonces finaliza.

La Figura 5 ilustra una visualización 500 de contexto de notificación, según un ejemplo. La visualización 500 de contexto de notificación es un ejemplo de una presentación de un contexto de un dispositivo solicitante según se presenta a un usuario de un dispositivo autorizante. La visualización 500 de contexto de notificación es un ejemplo de una presentación presentada por el proceso 400 de gestión de notificaciones descrito más arriba.

La visualización 500 de contexto de notificación muestra información asociada a una solicitud de acceso que se recibe de un dispositivo solicitante. La visualización 500 de contexto de notificación presenta información que se provee por el dispositivo solicitante, o información que se deriva según información asociada al dispositivo solicitante.

La visualización 500 de contexto de notificación tiene un título 502 que indica "SOLICITUD DE ACCESO

CUESTIONABLE RECIBIDA". Este título notifica al usuario del dispositivo de autorización que una solicitud de acceso se ha recibido para la cual se proveerá su aprobación o rechazo. La visualización 500 de contexto de notificación incluye información incluida en la solicitud de acceso. Información incluida en la solicitud de acceso incluye información en una línea 504 "DATOS", que, en este ejemplo, indica que la solicitud de acceso es para "DOCUMENTO A".

En general, una solicitud de acceso incluirá una dirección de Protocolo de Internet (IP) del dispositivo solicitante. En el ejemplo ilustrado, el proceso 400 de gestión de notificaciones determina un país asociado a la dirección IP especificada, y determina una ciudad en la cual probablemente se encuentre ubicada la dirección IP. Dicha información puede determinarse por cualquier técnica adecuada. La visualización 500 de contexto de notificación incluye una línea 506 "PAÍS DE IP DEL SOLICITANTE" que indica que la dirección IP del dispositivo solicitante se asocia a dispositivos en "PAÍS A". Una línea 508 "UBICACIÓN DE IP ESTIMADA DEL SOLICITANTE" indica que una ciudad "CIUDAD B" es una ubicación probable dentro de PAÍS A para el IP del dispositivo solicitante.

Otra información provista por el dispositivo solicitante que envía la solicitud de acceso incluye información presentada en una línea 512 "SISTEMA OPERATIVO DEL SOLICITANTE" que indica que la solicitud de acceso ha indicado que el sistema operativo del dispositivo solicitante es "DESCONOCIDO". En algunos ejemplos, el sistema operativo del dispositivo puede especificarse por el dispositivo solicitante o el sistema operativo puede determinarse por cualquier técnica adecuada. Una línea 412 "NOMBRE DE USUARIO DEL SOLICITANTE" indica que el nombre del usuario del dispositivo solicitante es "ABC" en este ejemplo. Una línea 414 "NÚMERO TELEFÓNICO DEL SOLICITANTE" indica que el número telefónico del usuario del dispositivo solicitante es "1234567".

La visualización 500 de contexto de notificación incluye un botón 520 "PERMITIR" y un botón 522 "RECHAZAR". Un usuario del dispositivo de autorización que presenta la visualización 500 de contexto de notificación puede seleccionar uno de estos botones como la respuesta de autorización que se recibe por el proceso 400 de gestión de notificaciones, descrito más arriba.

La Figura 6 es un diagrama de bloques de un dispositivo electrónico y componentes 600 asociados en el cual pueden implementarse los sistemas y métodos descritos en la presente memoria. En varios ejemplos, el dispositivo 652 electrónico puede ser un ejemplo de un dispositivo de comunicación bidireccional inalámbrico. El dispositivo 652 electrónico en varios ejemplos puede ser un dispositivo que lleva a cabo comunicaciones de datos, comunicaciones de datos y voz, comunicaciones de texto, varios otros tipos de comunicaciones, o combinaciones de estos. Dichos dispositivos electrónicos se comunican con una o más redes 650, las cuales pueden incluir capacidades de comunicaciones cableadas o inalámbricas para voz, texto, datos o combinaciones de estos. En un ejemplo, las redes 650 usan cualquier protocolo adecuado de comunicaciones cableadas o inalámbricas. Las comunicaciones de voz inalámbricas pueden llevarse a cabo usando un canal de comunicación inalámbrica analógico o digital. Las comunicaciones de datos permiten al dispositivo 652 electrónico comunicarse con otros sistemas informáticos en algunos ejemplos mediante Internet. Ejemplos de dispositivos electrónicos que pueden incorporar los sistemas y métodos descritos más arriba incluyen, por ejemplo, un dispositivo de mensajería de datos, un localizador bidireccional, un teléfono móvil con capacidades de mensajes de texto y datos, un dispositivo de Internet inalámbrico o un dispositivo de comunicación de datos que puede o puede no incluir capacidades de telefonía.

El dispositivo 652 electrónico ilustrado es un dispositivo electrónico a modo de ejemplo que incluye funciones de comunicaciones inalámbricas bidireccionales. Dichos dispositivos electrónicos pueden incorporar elementos del sistema de comunicación como, por ejemplo, un transmisor 610 inalámbrico, un receptor 612 inalámbrico y componentes asociados como, por ejemplo, uno o más elementos 614 y 616 de antena. Un procesador 608 de señales digitales (DPS, por sus siglas en inglés) lleva a cabo el procesamiento para extraer datos de señales inalámbricas recibidas y para generar señales que se transmitirán. El diseño particular del sistema de comunicación puede depender de la red de comunicación y protocolos de comunicaciones inalámbricas asociados con los cuales pretende funcionar el dispositivo.

El dispositivo 652 electrónico incluye un microprocesador 602 que controla el funcionamiento general del dispositivo 652 electrónico. El microprocesador 602 interactúa con los elementos del sistema de comunicaciones descrito más arriba y también interactúa con otros sistemas de dispositivo. En varios ejemplos, el dispositivo 652 electrónico puede incluir uno o más de varios componentes como, por ejemplo, un almacenamiento 606 de datos, memoria 604 de acceso aleatorio (RAM, por sus siglas en inglés), dispositivo 638 de entrada/salida (E/S) auxiliar, puerto 628 de datos, visualización 634, teclado 636, auricular 632, sistema 670 de reproducción de sonido de audio, micrófono 630, sistema 620 de comunicaciones de corto alcance, un sistema 622 de alimentación, otros sistemas, o combinaciones de estos.

Uno o más elementos de almacenamiento o suministro de energía como, por ejemplo, una batería 624, se conectan a un sistema 622 de alimentación para proveer energía a los circuitos del dispositivo 652 electrónico. El sistema 622 de alimentación incluye circuitos de distribución de alimentación para proveer energía al dispositivo 652 electrónico y también contiene circuitos de carga de batería para gestionar la recarga de la batería 624 (o circuitos para reponer energía a otro elemento de almacenamiento de energía). El sistema 622 de alimentación recibe energía eléctrica del suministro 654 de energía externa. El sistema 622 de alimentación puede conectarse al suministro 654 de energía externa a través de un conector de energía externa dedicado (no se muestra) o a través de conexiones de energía dentro del puerto 628 de datos. El sistema 622 de alimentación incluye un circuito de monitoreo de batería que es utilizable para proveer un estado de uno o más indicadores de estado de batería como, por ejemplo, capacidad

restante, temperatura, tensión, consumo de corriente eléctrica, y similar, a varios componentes del dispositivo 652 electrónico.

El puerto 628 de datos puede soportar comunicaciones de datos entre el dispositivo 652 electrónico y otros dispositivos a través de varios modos de comunicaciones de datos como, por ejemplo, transferencias de datos a alta velocidad en un circuito de comunicaciones ópticas. El puerto 628 de datos puede soportar comunicaciones con, por ejemplo, un ordenador externo u otro dispositivo. En algunos ejemplos, el puerto 628 de datos puede incluir conexiones de energía eléctrica para proveer energía eléctrica externamente provista al dispositivo 652 electrónico, entregar energía eléctrica del dispositivo 652 electrónico a otros dispositivos externamente conectados, o ambos. El puerto 628 de datos de, por ejemplo, un accesorio electrónico puede proveer energía a un circuito electrónico como, por ejemplo, microprocesador 602, y soportar el intercambio de datos entre el microprocesador 602 y un dispositivo electrónico remoto que se conecta a través del puerto 628 de datos.

La comunicación de datos a través del puerto 628 de datos permite a un usuario establecer preferencias a través del dispositivo externo o a través de una aplicación de software y extiende las capacidades del dispositivo al permitir el intercambio de información o software a través de conexiones directas entre el dispositivo 652 electrónico y fuentes de datos externas antes que mediante una red de comunicación de datos inalámbrica. Además de la comunicación de datos, el puerto 628 de datos provee energía al sistema 622 de alimentación para cargar la batería 624 o para suministrar energía a los circuitos electrónicos como, por ejemplo, microprocesador 602, del dispositivo 652 electrónico.

El software del sistema operativo usado por el microprocesador 602 se almacena en el almacenamiento 606 de datos. Ejemplos de almacenamiento 606 de datos pueden incluir, por ejemplo, memoria flash, dispositivos de almacenamiento magnético, otros elementos de almacenamiento de datos permanentes o no permanentes, o similar. Algunos ejemplos pueden usar almacenamiento 606 de datos que incluye una RAM soportada por batería u otros elementos de datos de almacenamiento permanente para almacenar sistemas operativos, otros programas ejecutables, o ambos. El software del sistema operativo, software de aplicaciones de dispositivo, o sus partes, pueden cargarse, de manera temporal, en un almacenamiento de datos no permanente como, por ejemplo, RAM 604. Los datos recibidos mediante señales de comunicación inalámbrica o a través de comunicaciones cableadas también pueden almacenarse en RAM 604.

El microprocesador 602, además de sus funciones de sistema operativo, puede ejecutar aplicaciones de software en el dispositivo 652 electrónico. Un conjunto de aplicaciones que controlan operaciones de dispositivo básicas, incluidas al menos aplicaciones de comunicación de datos y voz, puede instalarse en el dispositivo 652 electrónico durante la fabricación. En un ejemplo, programas y otros datos usados para soportar los procesos descritos más arriba pueden instalarse en la memoria del dispositivo 652 electrónico. Ejemplos adicionales de aplicaciones que pueden cargarse en el dispositivo pueden ser una aplicación de gestor de información personal (PIM, por sus siglas en inglés) que tiene la capacidad de organizar y gestionar elementos de datos relativos al usuario del dispositivo como, por ejemplo, entre otros, correo electrónico, eventos de calendario, correos de voz, citas, y elementos de tareas. Las aplicaciones pueden incluir las aplicaciones de base descritas más arriba, que pueden instalarse durante la fabricación o desde otra fuente fiable y verificada, junto con aplicaciones de usuario que pueden instalarse en cualquier momento.

Aplicaciones adicionales pueden también cargarse en el dispositivo 652 electrónico a través de, por ejemplo, la red 650 inalámbrica, un dispositivo 638 E/S auxiliar, puerto 628 de datos, sistema 620 de comunicaciones de corto alcance, o cualquier combinación de estas interfaces. Dichas aplicaciones pueden entonces instalarse por un usuario en la RAM 604 o un almacenamiento permanente para la ejecución por el microprocesador 602.

En un modo de comunicación de datos, una señal recibida como, por ejemplo, un mensaje de texto o descarga de página web se procesa por el sistema de comunicación, incluidos el receptor 612 inalámbrico y el transmisor 610 inalámbrico, y datos comunicados se proveen al microprocesador 602, que puede además procesar los datos recibidos. En algunos ejemplos, el dispositivo 652 electrónico incluye una visualización, puertos de salida, o combinaciones de estos. En dichos ejemplos, los datos recibidos pueden procesarse para su emisión a la visualización 634 o, de manera alternativa, a un dispositivo 638 E/S auxiliar, o puerto 628 de datos. En ejemplos del dispositivo 652 electrónico que incluyen un teclado 636 u otras instalaciones de entrada similares, un usuario del dispositivo 652 electrónico puede también componer elementos de datos como, por ejemplo, mensajes de correo electrónico, mediante el uso del teclado 636, que puede incluir un teclado alfanumérico completo o un teclado numérico tipo teléfono, en conjunto con la visualización 634 y posiblemente un dispositivo 638 E/S auxiliar. Dichos elementos compuestos pueden entonces transmitirse en una red de comunicación a través del sistema de comunicación.

Para las comunicaciones de voz, el funcionamiento general del dispositivo 652 electrónico es sustancialmente similar, excepto que las señales recibidas se proveen normalmente a un auricular 632 y las señales para la transmisión se producen, en general, por un micrófono 630. Sistemas E/S de voz o audio alternativos como, por ejemplo, un sistema de grabación de mensajes de voz, pueden también implementarse en el dispositivo 652 electrónico. Aunque la salida de señal de voz o audio se logra, en general, principalmente a través del auricular 632, en ejemplos de dispositivos 652 electrónicos que incluyen una visualización 634, la visualización 634 puede también usarse para proveer una indicación de la identidad de una parte que llama, la duración de una llamada de voz, u otra información relacionada con la llamada de voz, por ejemplo.

Dependiendo de las condiciones o estados del dispositivo 652 electrónico, pueden deshabilitarse una o más funciones particulares asociadas a un circuito de sistema, o puede deshabilitarse un circuito de sistema entero. Por ejemplo, si la temperatura de la batería es baja, entonces las funciones de voz pueden deshabilitarse, pero las comunicaciones de datos como, por ejemplo, correo electrónico, pueden aún permitirse en el sistema de comunicación.

Un sistema 620 de comunicaciones de corto alcance provee la comunicación de datos entre el dispositivo 652 electrónico y diferentes sistemas o dispositivos, los cuales no necesitan necesariamente ser dispositivos similares. Por ejemplo, el sistema 620 de comunicaciones de corto alcance incluye un dispositivo infrarrojo y circuitos y componentes asociados o un módulo de comunicación basado en radiofrecuencia como, por ejemplo, uno que soporta comunicaciones Bluetooth®, para proveer la comunicación con sistemas y dispositivos habilitados de manera similar, incluidas las comunicaciones de transferencia de archivos de datos descritas más arriba. El sistema de comunicaciones de corto alcance puede también incluir uno o más de los componentes para soportar las comunicaciones en enlaces inalámbricos como, por ejemplo, WiFi®, comunicaciones de campo cercano (NFC, por sus siglas en inglés), cualquier otro enlace de corto alcance, o combinaciones de estos.

Un lector 660 de medios puede conectarse a un dispositivo 638 E/S auxiliar para permitir, por ejemplo, la carga de un código de programa legible por ordenador de un producto de programa de ordenador al dispositivo 652 electrónico para su almacenamiento en la memoria 606 flash. Un ejemplo de un lector 660 de medios es una unidad óptica como, por ejemplo, una unidad CD/DVD, que puede usarse para almacenar datos en y leer datos de un medio legible por ordenador o producto de almacenamiento como, por ejemplo, un medio 662 de almacenamiento legible por ordenador. Ejemplos de medios de almacenamiento legibles por ordenador adecuados incluyen medios de almacenamiento óptico como, por ejemplo, un CD o DVD, medios magnéticos, o cualquier otro dispositivo de almacenamiento de datos adecuado. El lector 660 de medios puede, de manera alternativa, conectarse al dispositivo electrónico a través del puerto 628 de datos o el código de programa legible por ordenador puede, de manera alternativa, proveerse al dispositivo 652 electrónico a través de la red 650 inalámbrica.

Sistema de procesamiento de información

El presente objeto puede realizarse en hardware, software, o una combinación de hardware y software. Un sistema puede realizarse en una manera centralizada en un sistema de ordenador, o en una manera distribuida donde diferentes elementos se diseminan a lo largo de varios sistemas de ordenador interconectados. Cualquier tipo de sistema informático - u otro aparato adaptado para llevar a cabo los métodos descritos en la presente memoria - es adecuado. Una combinación típica de hardware y software puede ser un sistema de ordenador de propósito general con un programa de ordenador que, cuando se carga y ejecuta, controla el sistema informático de modo tal que lleva a cabo los métodos descritos en la presente memoria.

El presente objeto puede también realizarse en un producto de programa de ordenador, que comprende todas las características que permiten la implementación de los métodos descritos en la presente memoria, y que - cuando se carga en un sistema informático - puede llevar a cabo estos métodos. Programa de ordenador en el presente contexto significa cualquier expresión, en cualquier lenguaje, código o notación, de un conjunto de instrucciones destinadas a hacer que un sistema que tiene una capacidad de procesamiento de información lleve a cabo una función particular ya sea directamente o después de o ambas de las siguientes a) conversión a otro lenguaje, código o notación; y b) reproducción en una forma material diferente.

Cada sistema de ordenador puede incluir, entre otros, uno o más ordenadores y al menos un medio legible por ordenador que permite a un ordenador leer datos, instrucciones, mensajes o paquetes de mensajes, y otra información legible por ordenador del medio legible por ordenador. El medio legible por ordenador puede incluir un medio de almacenamiento legible por ordenador no transitorio que incorpora una memoria permanente como, por ejemplo, una memoria de solo lectura (ROM, por sus siglas en inglés), memoria flash, memoria de unidad de disco, CD-ROM, y otro almacenamiento permanente. Además, un medio de ordenador puede incluir almacenamiento no permanente como, por ejemplo, RAM, búferes, memoria caché y circuitos de red. Además, el medio legible por ordenador puede comprender información legible por ordenador en un medio en estado transitorio como, por ejemplo, un enlace de red y/o una interfaz de red, incluida una red cableada o una red inalámbrica, que permiten a un ordenador leer dicha información legible por ordenador.

Ejemplos no restrictivos

Aunque se han descrito realizaciones específicas del objeto, las personas con experiencia ordinaria en la técnica comprenderán que pueden llevarse a cabo cambios en las realizaciones específicas sin apartarse del alcance del objeto descrito. El alcance de la descripción no se limitará, por lo tanto, a las realizaciones específicas, y se pretende que las reivindicaciones anexas cubran todas las aplicaciones, modificaciones y realizaciones dentro del alcance de la presente descripción.

REIVINDICACIONES

1. Un método, que comprende:

acumular un historial de solicitudes de acceso para datos solicitados, el historial de solicitudes de acceso comprendiendo respectivos contextos de dispositivos (130) solicitantes que realizan las solicitudes de acceso;

determinar, según un análisis del respectivo contexto contenido en cada solicitud de acceso en el historial de solicitudes de acceso, un patrón de acceso para los datos solicitados;

recibir (302), después de acumular el historial de solicitudes de acceso, una solicitud de acceso presente de un dispositivo solicitante para acceder a los datos solicitados;

determinar un contexto para el dispositivo solicitante que envía la presente solicitud de acceso;

determinar (308) una desviación entre el contexto para el dispositivo solicitante que envía la presente solicitud de acceso y el patrón de acceso;

comparar, según la determinación de la desviación, el contexto del presente dispositivo solicitante con contextos definidos en el patrón de acceso;

enviar (314), según la comparación, una notificación que comprende el contexto para el dispositivo solicitante a un dispositivo (120) de autorización asociado a los datos solicitados, en donde el dispositivo de autorización recibe (316, 406) una respuesta de autorización para la presente solicitud de acceso de un usuario del dispositivo de autorización, y

permitir (324) el acceso a los datos solicitados según la respuesta a la notificación que se recibe (402) del dispositivo de autorización.

2. El método de la reivindicación 1, en donde los datos solicitados se protegen por al menos una de gestión de derechos digitales o gestión de derechos de información, y

en donde permitir el acceso comprende conceder una clave en virtud de la gestión de derechos digitales o gestión de derechos de información.

3. El método de la reivindicación 1, que además comprende recibir, durante la configuración de protección para los datos solicitados, un identificador del dispositivo (120) de autorización asociado a los datos solicitados.

4. Un dispositivo (652), que comprende:

un procesador (602) de contexto que, cuando está funcionando:

acumula un historial de solicitudes de acceso para datos solicitados, el historial de solicitudes de acceso comprendiendo respectivos contextos de dispositivos (130) solicitantes que realizan las solicitudes de acceso;

determina (302), según un análisis del respectivo contexto contenido en cada solicitud de acceso en el historial de solicitudes de acceso, un patrón de acceso para los datos solicitados,

recibe, después de acumular el historial de solicitudes de acceso, una solicitud de acceso presente de un dispositivo solicitante para acceder a los datos solicitados;

determina un contexto para el dispositivo solicitante que envía la presente solicitud de acceso para los datos solicitados;

determina (308) una desviación entre el contexto para el dispositivo solicitante que envía la presente solicitud de acceso y el patrón de acceso;

compara, según la determinación de la desviación, el contexto del presente dispositivo solicitante con contextos definidos en el patrón de acceso;

envía (314), según la comparación, una notificación que comprende el contexto para el dispositivo solicitante a un dispositivo (120) de autorización asociado a los datos solicitados, en donde el dispositivo de autorización recibe (316, 406) una respuesta de autorización para la presente solicitud de acceso de un usuario del dispositivo de autorización; y

permite (324) el acceso a los datos solicitados según la respuesta a la notificación que se recibe (402) del dispositivo de autorización; y

una interfaz de datos que, cuando está funcionando, recibe la presente solicitud de acceso del dispositivo solicitante.

5. El dispositivo de la reivindicación 4, en donde los datos solicitados se protegen por al menos una de gestión de derechos digitales o gestión de derechos de información, y

en donde el procesador (602) de contexto, cuando está funcionando, permite el acceso al conceder una clave en virtud de la gestión de derechos digitales o gestión de derechos de información.

6. Un medio de almacenamiento legible por ordenador que tiene un código de programa legible por ordenador allí incorporado, el código de programa legible por ordenador comprendiendo instrucciones para llevar a cabo el método de cualquiera de las reivindicaciones 1 a 3.

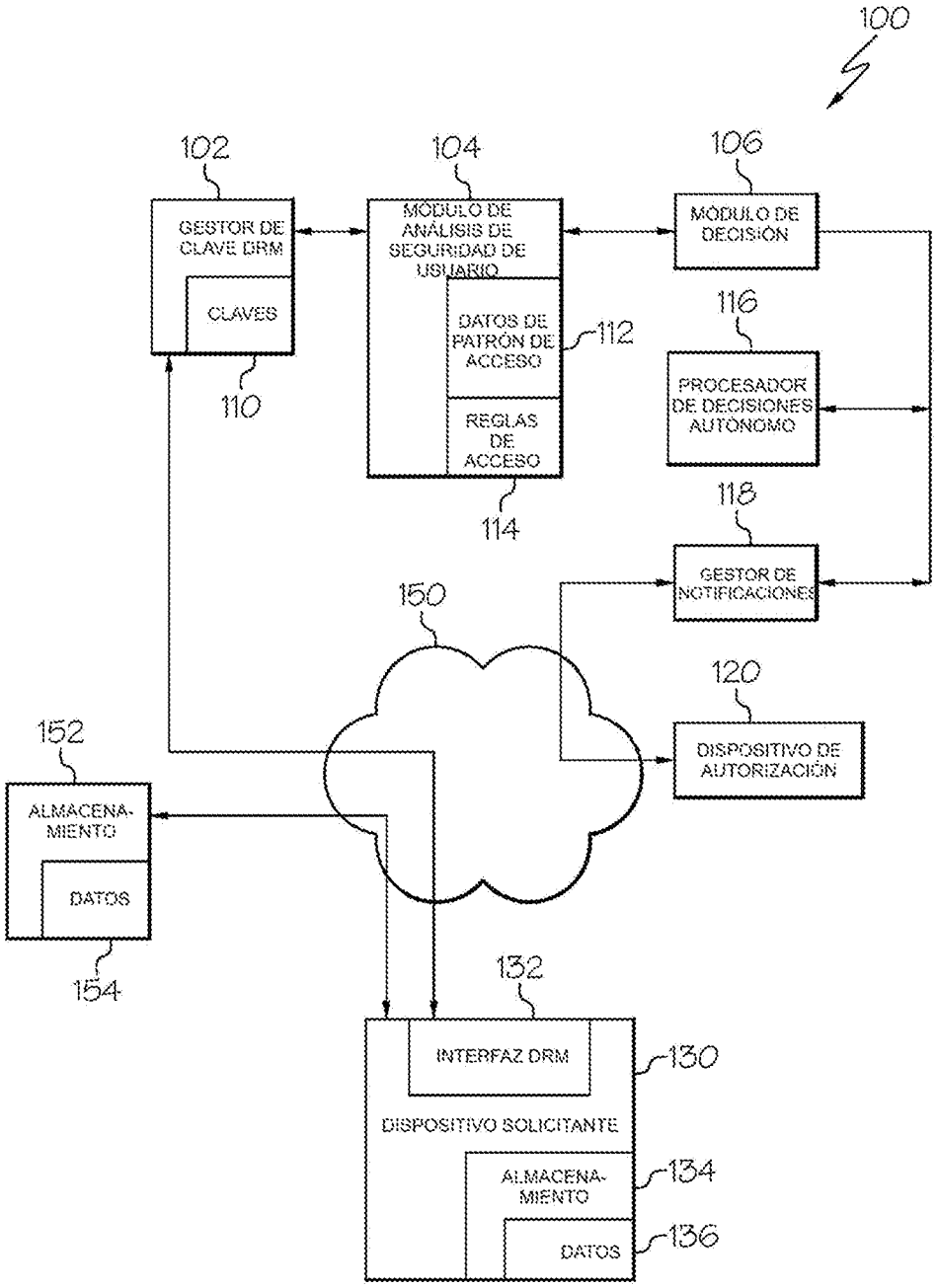
100
102
GESTOR DE CLAVE DRM
CLAVES
110
104
MÓDULO DE ANÁLISIS DE SEGURIDAD DE USUARIO
DATOS DE PATRÓN DE ACCESO
112
REGLAS DE ACCESO
114
106
MÓDULO DE DECISIÓN
116
PROCESADOR DE DECISIONES AUTÓNOMO
118
GESTOR DE NOTIFICACIONES
150
120
DISPOSITIVO DE AUTORIZACIÓN
152
ALMACENA-MIENTO
DATOS
154
132
INTERFAZ DRM
130
DISPOSITIVO SOLICITANTE
ALMACENA-MIENTO
134
DATOS
136

FIG. 1

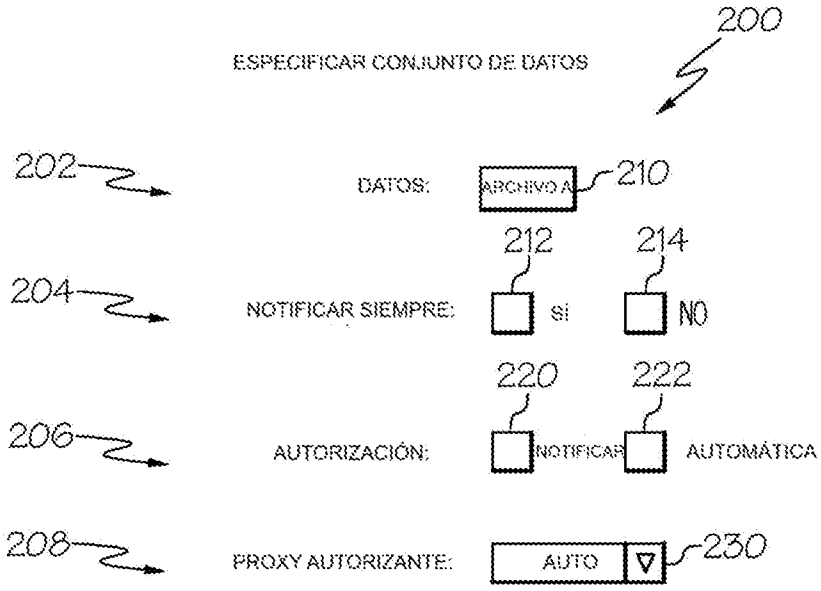
ESPECIFICAR CONJUNTO DE DATOS
200
202
DATOS:
ARCHIVO A
210
212
214
204
NOTIFICAR SIEMPRE:
SÍ
NO
220
222
206
AUTORIZACIÓN:
NOTIFICAR
AUTOMÁTICA
208
PROXY AUTORIZANTE:
AUTO
230

FIG. 2

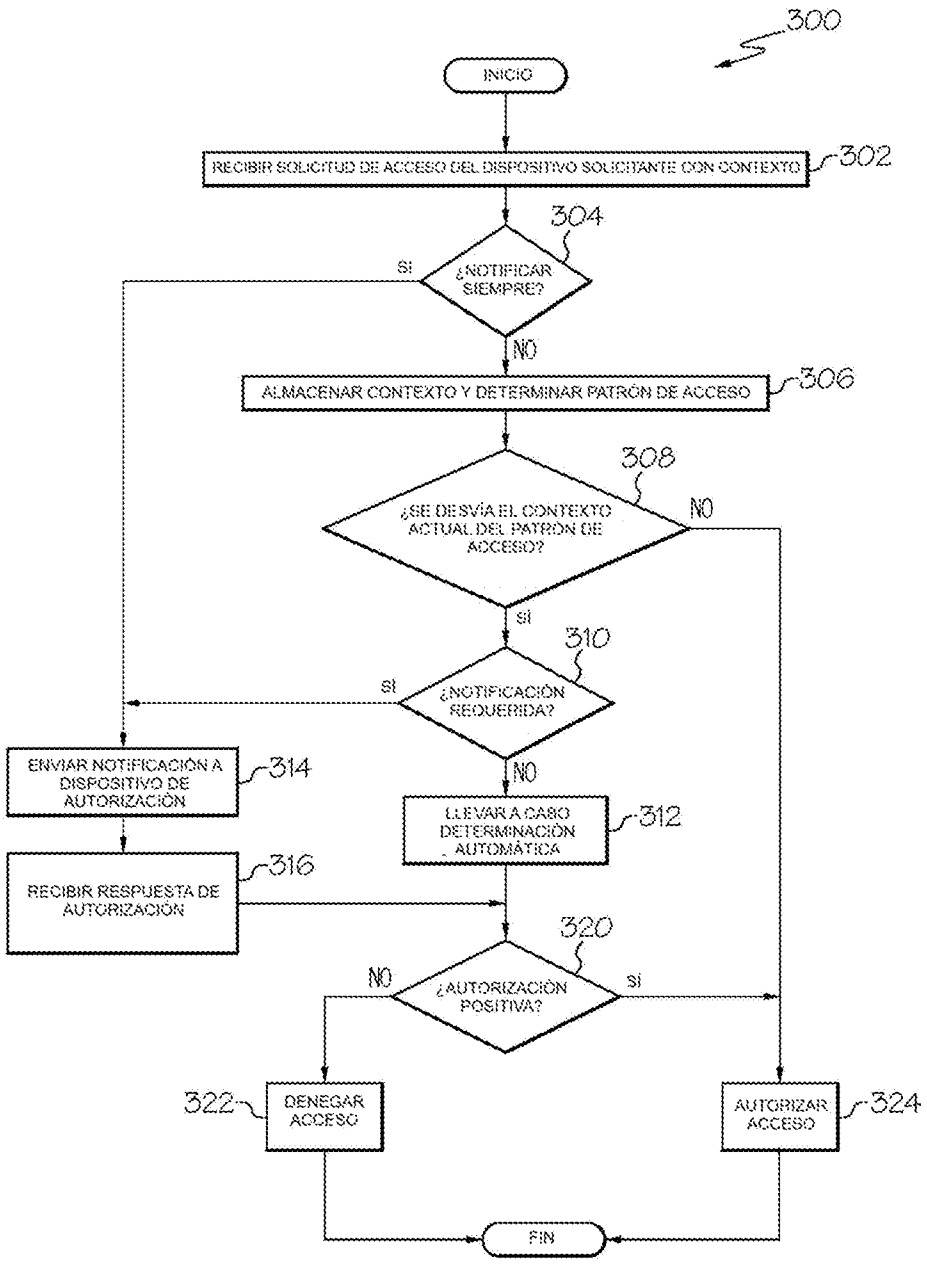
300
INICIO
RECIBIR SOLICITUD DE ACCESO DEL DISPOSITIVO SOLICITANTE CON CONTEXTO
302
304
¿NOTIFICAR SIEMPRE?
SI
NO
ALMACENAR CONTEXTO Y DETERMINAR PATRÓN DE ACCESO
306
308
¿SE DESVÍA EL CONTEXTO ACTUAL DEL PATRÓN DE ACCESO?
NO
SI
310
¿NOTIFICACIÓN REQUERIDA?
SI
NO
ENVIAR NOTIFICACIÓN A DISPOSITIVO DE AUTORIZACIÓN
314
LLEVAR A CABO DETERMINACIÓN AUTOMÁTICA
312
RECIBIR RESPUESTA DE AUTORIZACIÓN
316
320
¿AUTORIZACIÓN POSITIVA?
NO
SI
322
DENEGAR ACCESO
AUTORIZAR ACCESO
324
FIN

FIG. 3

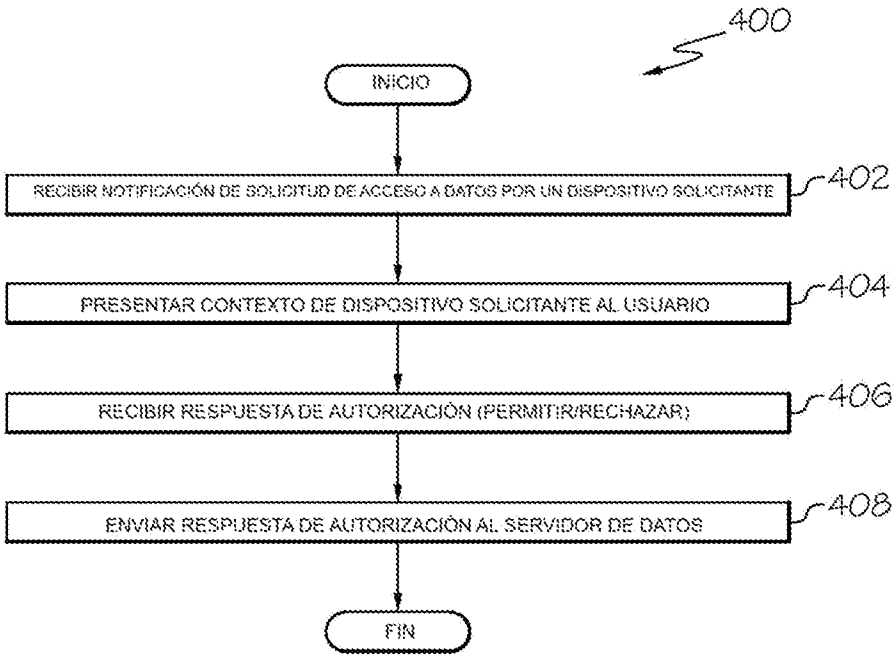
400
INICIO
RECIBIR NOTIFICACIÓN DE SOLICITUD DE ACCESO A DATOS POR UN DISPOSITIVO SOLICITANTE
402
PRESENTAR CONTEXTO DE DISPOSITIVO SOLICITANTE AL USUARIO
404
RECIBIR RESPUESTA DE AUTORIZACIÓN (PERMITIR/RECHAZAR)
406
ENVIAR RESPUESTA DE AUTORIZACIÓN AL SERVIDOR DE DATOS
408
FIN

FIG. 4

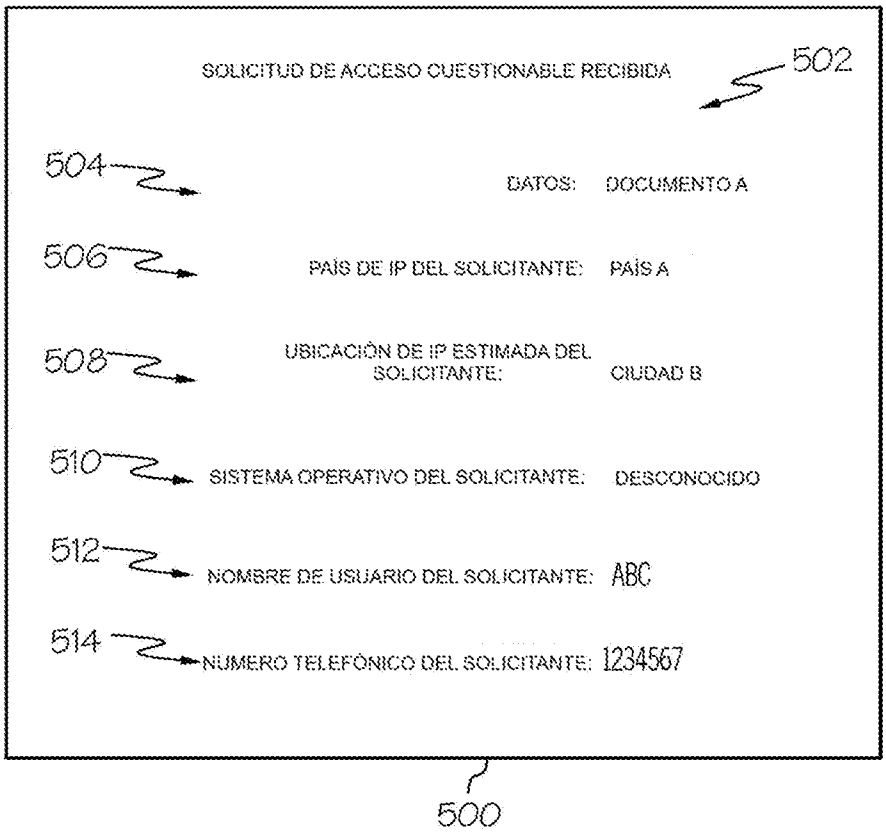
SOLICITUD DE ACCESO CUESTIONABLE RECIBIDA
502
504
DATOS: DOCUMENTO A
506
PAÍS DE IP DEL SOLICITANTE: PAÍS A
508
UBICACIÓN DE IP ESTIMADA DEL SOLICITANTE: CIUDAD B
510
SISTEMA OPERATIVO DEL SOLICITANTE: DESCONOCIDO
512
NOMBRE DE USUARIO DEL SOLICITANTE: ABC
514
NÚMERO TELEFÓNICO DEL SOLICITANTE: 1234567
500

FIG. 5

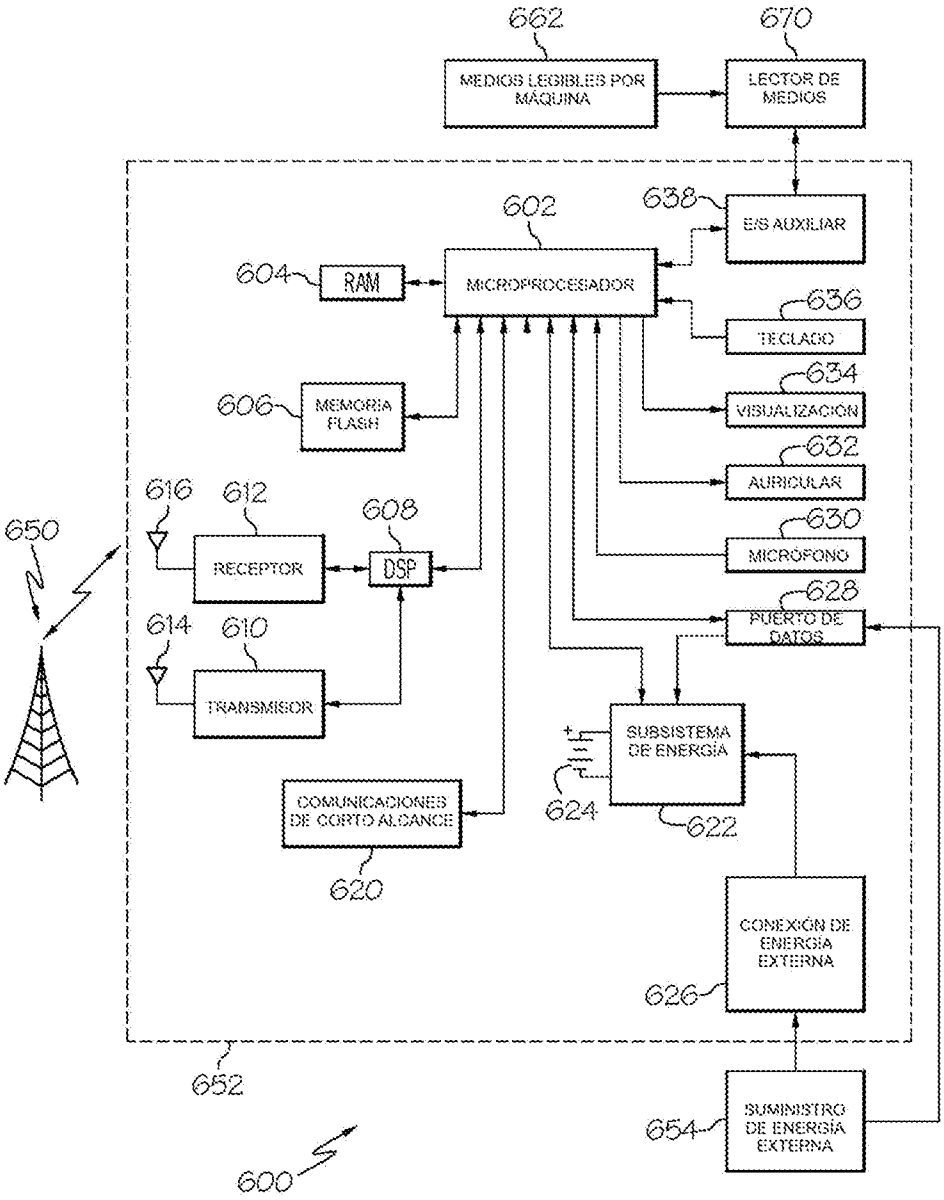
662
MEDIOS LEGIBLES POR MÁQUINA
670
LECTOR DE MEDIOS
638
E/S AUXILIAR
602
604
RAM
MICROPROCESADOR
636
TECLADO
634
VISUALIZACIÓN
606
MEMORIA FLASH
632
AURICULAR
616
612
608
650
RECEPTOR
DSP
630
MICRÓFONO
628
PUERTO DE DATOS
614
610
TRANSMISOR
SUBSISTEMA DE ENERGÍA
624
622
COMUNICACIONES DE CORTO ALCANCE
620
CONEXIÓN DE ENERGÍA EXTERNA
626
652
654
SUMINISTRO DE ENERGÍA EXTERNA
600

FIG. 6