(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 800 900**

(51) Int. CI.:

H04W 12/02 (2009.01)
G06F 21/62 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.03.2015 PCT/EP2015/054370**

(87) Fecha y número de publicación internacional: **08.10.2015 WO15150006**

(96) Fecha de presentación y número de la solicitud europea: **03.03.2015 E 15709644 (7)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 3127038**

(54) Título: **Método y sistema para proteger y/o anonimizar la identidad de usuario y/o los datos de usuario de un abonado de un servicio de protección de datos, red de comunicación móvil, programa y producto de programa de ordenador**

(30) Prioridad:

31.03.2014 EP 14162870

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.01.2021

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

THOMAS, GRAHAM

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método y sistema para proteger y/o anonimizar la identidad de usuario y/o los datos de usuario de un abonado de un servicio de protección de datos, red de comunicación móvil, programa y producto de programa de ordenador

ANTECEDENTES

La presente invención se refiere a un método para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos.

Además, la presente invención se refiere a un sistema para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos.

Adicionalmente, la presente invención se refiere a una red de comunicación móvil adecuada para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos.

Algunos servicios de terceros, por ejemplo, los llamados servicios sensibles al contexto, generalmente usan elementos contextuales para aprender sobre el comportamiento y la situación de un usuario, en donde se pueden proporcionar recomendaciones inteligentes al usuario. Por ejemplo, un servicio puede solicitar acceder al correo electrónico y otros datos de usuario con el fin de actuar como asistente personal. Sin embargo, los servicios de terceros requieren información personal del usuario con el fin de proporcionar el servicio dirigido al usuario. Por lo tanto, la protección de la privacidad del usuario es relativamente baja debido a que las empresas asociadas con los servicios de terceros pueden hacer un uso indebido de la información personal o venderla a otras organizaciones. El documento US 2014/0059693 A1 describe un método para gestionar la privacidad de la información de cuenta bancaria personal, que implica asociar el identificador de envío con un identificador de usuario, donde la información de la dirección de un usuario anónimo se obtiene de una entidad de envío.

COMPENDIO

Un objeto de la presente invención es proporcionar un método, un sistema y una red de comunicación móvil para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos, de modo que se mejora la comodidad del usuario con respecto a servicios de terceros que se proporcionan a través de la red de telecomunicaciones.

El objeto de la presente invención se logra por un método para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos,

en donde se accede al servicio de protección de datos, a través de una red de telecomunicaciones, por medio de un dispositivo informático del abonado del servicio de protección de datos, el dispositivo informático que está conectado a la red de telecomunicaciones,

en donde en caso de que el dispositivo informático acceda a un servicio de terceros a través de la red de telecomunicaciones, el servicio de terceros recibe datos relacionados con el usuario, los datos relacionados con el usuario siendo datos relacionados con la identidad del usuario y/o los datos de usuario, en donde el acceso al servicio de terceros a través del servicio de protección de datos implica una transmisión de los datos relacionados con el usuario de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respecto al servicio de terceros

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros, o
- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado, en donde el servicio de protección de datos crea un pasaporte digital dependiendo de la identidad del usuario y/o datos del usuario del abonado, y además dependiendo de la información de autorización del abonado, en donde el abonado proporciona la información de autorización para el servicio de terceros.

Según la presente invención es, por lo tanto, ventajosamente posible utilizar servicios de terceros, que generalmente requieren una identidad de usuario y/o unos datos de usuario (datos personales), de modo que se mejora la comodidad del usuario, en particular con respecto a la seguridad de la información y/o la protección de la privacidad. Preferiblemente, la seguridad de la información se mejora con respecto a los datos de usuario y/o la identidad del usuario debido a que los servicios de terceros pueden usarse sin o solo proporcionando parcialmente los datos de usuario y/o la identidad del usuario (en forma de datos relacionados con el usuario) al servicio de terceros. El uso indebido de la información personal por parte de un tercero por lo tanto se inhibe ventajosamente o al menos se contiene. Preferiblemente, al servicio de protección de datos también se le llama, por lo tanto, un proveedor de confianza. Por ejemplo, el servicio de terceros es un servicio de pagos, un servicio de aplicación o un servicio de comercio electrónico.

Según una realización preferida de la presente invención, para una primera parte de la identidad del usuario y/o los datos del usuario, los datos relacionados con el usuario comprenden el texto plano de la identidad del usuario y/o los datos del usuario, y en donde para una segunda parte de la identidad del usuario y/o los datos del usuario, se evita la transmisión al servicio de terceros, o los datos relacionados con el usuario son datos modificados con respecto a la segunda parte de la identidad del usuario y/o los datos del usuario.

Según la presente invención es, por lo tanto, ventajosamente posible proporcionar al menos la segunda parte de la identidad del usuario y/o los datos de usuario al servicio de terceros por medio de un método seguro. Por ejemplo, el servicio de protección de datos comparte con el servicio de terceros la primera parte (de la identidad del usuario y/o los datos del usuario) abiertamente y la segunda parte (de la identidad del usuario y/o los datos del usuario) en un formato protegido.

Según una realización preferida de la presente invención, la identidad del usuario y/o los datos de usuario están completamente protegidos y/o anonimizados con respecto al servicio de terceros

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros, o
- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado.

Según la presente invención es, por lo tanto, ventajosamente posible proporcionar la identidad del usuario y/o los datos de usuario completos al servicio de terceros por medio de un método seguro. Por ejemplo, el servicio de protección de datos comparte con el servicio de terceros todos los datos, en un formato protegido.

Dentro del contexto de la invención presentada, preferiblemente el abonado del dispositivo informático selecciona, al menos, un primer o un segundo nivel de seguridad, con respecto al acceso del servicio de terceros a los datos relacionados con el usuario. Preferiblemente, cuando se selecciona el primer nivel de seguridad (nivel conserje), la identidad del usuario y/o los datos de usuario están completamente protegidos y/o anonimizados con respecto al servicio de terceros. Preferiblemente, cuando se selecciona el segundo nivel de seguridad (nivel protegido), solo una parte de la identidad del usuario y/o los datos de usuario están protegidos y/o anonimizados con respecto al servicio de terceros.

Según una realización preferida de la presente invención, la red de telecomunicaciones es una red de comunicación móvil, y el dispositivo informático es un dispositivo informático móvil, especialmente un teléfono móvil, un teléfono inteligente, una tableta u otro dispositivo informático portátil.

Según la presente invención es, por lo tanto, ventajosamente posible proporcionar el método para proteger y/o anonimizar la identidad del usuario y/o los datos de usuario del abonado del servicio de protección de datos de modo que además se mejora la comodidad del usuario.

Según una realización preferida de la presente invención, el servicio de terceros es una aplicación proporcionada al dispositivo informático, en donde la aplicación se ejecuta en el dispositivo informático o en un nodo de red de la red de telecomunicaciones, en donde al acceder al servicio de terceros a través del servicio de protección de datos, se modifica el comportamiento de la aplicación con respecto a la transmisión de los datos relacionados con el usuario, de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respecto al servicio de terceros.

Según la presente invención es, por lo tanto, ventajosamente posible modificar el comportamiento de la aplicación por medio de la aplicación de una estrategia de respuesta y/o de permiso. Preferiblemente, el comportamiento de la aplicación se modifica dependiendo del método de respuesta y/o de permiso que se lleve a cabo.

Según una realización preferida de la presente invención, el servicio de protección de datos comprende un sistema de respuesta para llevar a cabo el método de respuesta, en donde el servicio de terceros transmite un mensaje de solicitud al sistema de respuesta, estando el mensaje de solicitud configurado para solicitar los datos de usuario y/o la identidad del usuario asociados con el abonado del servicio protección de datos, en donde el sistema de respuesta transmite un mensaje de respuesta en respuesta al mensaje de solicitud, en donde el mensaje de respuesta comprende los datos relacionados con el usuario de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respecto al servicio de terceros.

Según la presente invención es, por lo tanto, ventajosamente posible ocultar eficientemente la identidad del usuario y/o los datos de usuario del servicio de terceros. Preferiblemente, los datos relacionados con el usuario se configuran de modo que el servicio de terceros recibe la información solicitada sin que se compartan los datos del perfil central del abonado. Por ejemplo, los datos de usuario pueden estar relacionados con el cumpleaños del abonado. El mensaje de respuesta puede comprender los datos relacionados con el usuario en forma de una fecha, por ejemplo, 20 de mayo, en lugar de la fecha de nacimiento.

Según una realización preferida de la presente invención, el servicio de protección de datos se configura de modo que el abonado puede registrarse o iniciar sesión con el servicio de protección de datos utilizando el dispositivo informático. En particular, el servicio de protección de datos proporciona una interfaz de inicio de sesión para el abonado. Preferiblemente, la interfaz de inicio de sesión es una interfaz gráfica de usuario que comprende un icono, por ejemplo, un icono TrustMe, que se utiliza para iniciar sesión. Preferiblemente, se genera una cuenta de usuario para el abonado, en donde los detalles personales y/u otros detalles de configuración se almacenan de modo que el abonado no necesita introducir la identidad del usuario y/o los datos de usuario cada vez que el abonado inicia la sesión en el servicio de protección de datos. Es, por lo tanto, ventajosamente posible mejorar la comodidad del usuario, en particular con respecto a la transmisión de los datos relacionados con el usuario, al servicio de terceros.

Según una realización preferida de la presente invención, el método comprende la anonimización de la identidad del usuario y los datos de usuario de modo que, al analizar los datos relacionados con el usuario transmitidos al servicio de terceros, se oculta la identidad del usuario asociada con el dispositivo informático.

Según la presente invención es, por lo tanto, ventajosamente posible proteger y/o anonimizar la identidad del usuario y/o los datos de usuario del abonado del servicio de protección de datos, de modo que se mejora la comodidad del usuario con respecto al acceso a servicios de terceros proporcionado a través de la red de telecomunicaciones.

La presente invención también se refiere a un sistema para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos, el sistema que comprende el servicio de protección de datos, una red de telecomunicaciones y un dispositivo informático,
en donde el sistema se configura de modo que se accede al servicio de protección de datos, a través de la red de telecomunicaciones, por medio del dispositivo informático del abonado del servicio de protección de datos, el dispositivo informático que se conecta a la red de telecomunicaciones,
en donde el sistema se configura de modo que en caso de que el dispositivo informático acceda a un servicio de terceros a través de la red de telecomunicaciones, el servicio de terceros recibe los datos relacionados con el usuario, siendo los datos relacionados con el usuario datos relacionados con la identidad del usuario y/o los datos del usuario, en donde el sistema se configura de modo que el acceso al servicio de terceros a través del servicio de protección de datos implica una transmisión de los datos relacionados con el usuario, de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respecto al servicio de terceros

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros, o
- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado, en donde el servicio de protección de datos se configura para crear un pasaporte digital dependiendo de la identidad del usuario y/o los datos de usuario del abonado y además dependiendo de la información de autorización del abonado, en donde el abonado proporciona la información de autorización para el servicio de terceros.

Según la presente invención es, por lo tanto, ventajosamente posible proteger y/o anonimizar la identidad del usuario y/o los datos de usuario del abonado de un servicio de protección de datos, de modo que se mejora la comodidad del usuario con respecto al acceso de servicios de terceros proporcionado a través de la red de telecomunicaciones. En particular, se inhibe el uso indebido de los datos personales. El sistema permite al abonado utilizar los servicios de terceros que requieren el uso de los datos relacionados con el usuario bajo condiciones mejoradas de seguridad de la información.

Según una realización preferida de la presente invención, el sistema se configura de modo que para una primera parte de la identidad del usuario y/o los datos de usuario, los datos relacionados con el usuario comprenden el texto plano de la identidad del usuario y/o los datos de usuario, y en donde el sistema se configura de modo que para una segunda parte de la identidad del usuario y/o los datos de usuario, se evita la transmisión al servicio de terceros, o los datos relacionados con el usuario son datos modificados con respecto a la segunda parte de la identidad del usuario y/o los datos de usuario.

Según la presente invención es, por lo tanto, ventajosamente posible proporcionar los datos relacionados con el usuario al servicio de terceros, de modo que el servicio de terceros recibe solo la primera parte de los datos de usuario y/o la identidad del usuario en texto plano. Por lo tanto, se alcanza un segundo nivel de seguridad (nivel protegido).

Según una realización preferida de la presente invención, el sistema se configura de modo que la identidad del usuario y/o los datos de usuario están completamente protegidos y/o anonimizados con respecto al servicio de terceros

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros, o

- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado.

Según la presente invención es, por lo tanto, ventajosamente posible proporcionar los datos relacionados con el usuario al servicio de terceros de modo que el servicio de terceros recibe los datos de usuario y/o la identidad de usuario completos de una forma segura. Por lo tanto, se alcanza un primer nivel de seguridad (nivel conserje).

Según una realización preferida de la presente invención, la red de telecomunicaciones es una red de comunicación móvil, y el dispositivo informático es un dispositivo informático móvil, especialmente un teléfono móvil, un teléfono inteligente, una tableta u otro dispositivo informático portátil.

Según la presente invención es, por lo tanto, ventajosamente posible proporcionar el método para proteger y/o anonimizar la identidad del usuario y/o los datos de usuario del abonado del servicio de protección de datos de modo que además se mejora la comodidad del usuario.

Además, la presente invención se refiere a una red de comunicación móvil adecuada para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos en un sistema, según la presente invención.

Además, la presente invención se refiere a un programa que comprende código de programa legible por un ordenador que, cuando se ejecuta en un ordenador o en un dispositivo informático o en un componente de red de una red de telecomunicaciones o en parte en un dispositivo informático y en parte en un componente de red de una red de telecomunicaciones, hace que el ordenador o el dispositivo informático y/o el componente de red de la red de telecomunicaciones ejecuten un método, según la presente invención.

Además, la presente invención se refiere a un producto de programa de ordenador para usar un dispositivo de comunicación de tipo máquina con una red de telecomunicaciones, el producto de programa de ordenador que comprende un programa de ordenador almacenado en un medio de almacenamiento, el programa de ordenador que comprende el código de programa que, cuando se ejecuta en un ordenador o en un dispositivo informático o en un componente de red de una red de telecomunicaciones o en parte en un dispositivo informático y en parte en un componente de red de una red de telecomunicaciones, hace que el ordenador o el dispositivo informático y/o el componente de red de la red de telecomunicaciones ejecuten un método, según la presente invención.

Estas y otras características, rasgos y ventajas de la presente invención llegarán a ser evidentes a partir de la siguiente descripción detallada, tomada en conjunto con los dibujos adjuntos, que ilustran, a modo de ejemplo, los principios de la invención. La descripción se da solo a modo de ejemplo, sin limitar el alcance de la invención. Las figuras de referencia citadas a continuación se refieren a los dibujos adjuntos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 ilustra esquemáticamente un sistema según la presente invención.

DESCRIPCIÓN DETALLADA

La presente invención se describirá con respecto a realizaciones particulares y con referencia a ciertos dibujos, pero la invención no se limita a los mismos, sino solo por las reivindicaciones. Los dibujos descritos son solo esquemáticos y no limitativos. En los dibujos, con fines ilustrativos, el tamaño de algunos de los elementos puede estar exagerado y no dibujado a escala.

Donde se usa un artículo indefinido o definido cuando se refiere a un sustantivo singular, por ejemplo, “un”, "una", “el”, “la", esto incluye el plural de ese sustantivo a menos que específicamente se indique algo más.

Además, los términos primero, segundo, tercero y similares, en la descripción y en las reivindicaciones, se utilizan para distinguir entre elementos similares y no necesariamente para describir un orden secuencial o cronológico. Debe entenderse que los términos que se utilizan así, son intercambiables bajo circunstancias apropiadas y que las realizaciones de la invención descritas en la presente memoria son capaces de operar en otras secuencias distintas de las descritas o ilustradas en la presente memoria.

En la Figura 1, se ilustra esquemáticamente un sistema según la presente invención. El sistema se configura para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos 200. El sistema comprende el servicio de protección de datos. 200, una red de telecomunicaciones 100 y un dispositivo informático 20.

Según la presente invención, la red de telecomunicaciones 100 es preferiblemente una red de telecomunicaciones basada en el Protocolo de Internet (IP) 100. La red de telecomunicaciones 100 puede incluir cualquier red informática fija y/o móvil, por ejemplo, Internet y/o cualquier red telefónica.

El dispositivo informático 20 es un dispositivo informático del abonado del servicio de protección de datos 200. El dispositivo informático 20 está conectado a la red de telecomunicaciones 100. El dispositivo informático 20 es preferiblemente un ordenador personal u ordenador móvil, por ejemplo, una tableta o un teléfono inteligente o cualquier otro dispositivo informático.

El sistema se configura de modo que se accede al servicio de protección de datos 200, a través de la red de telecomunicaciones 100, por medio del dispositivo informático 20 del abonado del servicio de protección de datos 200. Preferiblemente el abonado - que en la presente memoria también se le llama usuario del dispositivo informático 20 - se registra en el servicio de protección de datos 200, en donde se configura una cuenta personal para el usuario. El servicio de protección de datos 200 se configura para crear un pasaporte digital dependiendo de los datos de usuario y/o la identidad del usuario (datos personales) y además dependiendo de la información de autorización del usuario. El usuario proporciona la información de autorización (por ejemplo, un permiso o nivel de acceso) para el servicio de terceros 300. En particular, el pasaporte digital es controlado por el usuario del dispositivo informático 20 y puede actualizarse con el paso del tiempo.

El sistema se configura de modo que en caso de que el dispositivo informático 20 acceda a un servicio de terceros 300 a través de la red de telecomunicaciones 100, el servicio de terceros 300 recibe los datos relacionados con el usuario. Los datos relacionados con el usuario son datos relacionados con la identidad del usuario y/o los datos de usuario. Los datos de usuario y/o la identidad del usuario incluyen, por ejemplo, al menos uno de los siguientes: nombre, dirección del domicilio, dirección del domicilio laboral, fecha de nacimiento, sexo, estado civil, detalles familiares, detalles de salud, detalles de redes sociales, detalles de correo electrónico, detalles de calendario/contactos, detalles bancarios, otros detalles de proveedores de servicios, por ejemplo, aerolíneas, compañías de seguros, compañías de comercio electrónico, ubicación, dispositivos, preferencias personales (perfil), favoritos de internet/marcadores y uso, preferencias de seguridad. También será posible almacenar la identidad digital del abonado. Preferiblemente, el servicio de protección de datos 200 se configura de modo que la identidad de usuario y/o los datos de usuario puedan agregarse al pasaporte digital, por ejemplo, en forma de campos de datos. Preferiblemente, o bien el servicio de terceros 300 especifica uno o más campos de datos (en caso de que se requiera un elemento de datos que aún no está comprendido en el pasaporte digital) o bien el usuario introduce uno o más campos de datos. El servicio de protección de datos 200 es accesible desde cualquier dispositivo informático 20 conectado a la red de telecomunicaciones 100.

Preferiblemente, el servicio de protección de datos 200 comprende una interfaz de aplicación para la comunicación con un desarrollador de un servicio de terceros 300. Preferiblemente, la interfaz de la aplicación se configura para conectar el servicio de terceros 300 (por ejemplo, cualquier aplicación o servicio de internet) al servicio de protección de datos 200, de modo que el servicio de terceros 300 está certificado como vinculado al servicio de protección de datos 200. Preferiblemente, el servicio de protección de datos se configura para permitir o denegar el acceso a servicios de terceros. Por lo tanto, es ventajosamente posible excluir servicios ilegales o que estén en una lista negra.

Según una realización del sistema, el sistema se configura de modo que el acceso al servicio de terceros 300 a través del servicio de protección de datos 200 implica una transmisión de los datos relacionados con el usuario de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respecto al servicio de terceros 300, por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros 300. Según otra realización del sistema, el sistema se configura de modo que el acceso al servicio de terceros 300 a través del servicio de protección de datos 200 implica una transmisión de los datos relacionados con el usuario, de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respeto al servicio de terceros 300 por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros 300 - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado. Preferiblemente, datos modificados significa que se elimina cualquier asociación directa del abonado con los datos de usuario y/o la identidad del usuario, en donde los datos relacionados con el usuario se proporcionan en una forma que pueden ser utilizados por el servicio de terceros. Preferiblemente, el abonado está, por lo tanto, habilitado para controlar si los datos de usuario y/o la identidad del usuario se comparten con un servicio de terceros 300. En particular, el abonado está habilitado para configurar el servicio de protección de datos 200, de modo que los datos de usuario y/o la identidad del usuario se comparten al menos parcialmente abiertamente o se comparten al menos parcialmente de forma segura.

Preferiblemente, se generan los datos relacionados con el usuario dependiendo de los datos de usuario y/o la identidad del usuario utilizando un método basado en solicitud, un método de identidad protegida y/o un método basado en permisos.

En caso de que se utilice el método basado en solicitud, el servicio de terceros 300 solicita datos relacionados con el usuario, los datos relacionados con el usuario que se solicitan al servicio de protección de datos 200, por ejemplo, a través de la interfaz de la aplicación. Dependiendo de la solicitud de datos relacionados con el usuario por el servicio de terceros, el servicio de protección de datos 200 solicita la información de autorización relacionada con el servicio de terceros 300 al abonado en el dispositivo informático 20. Según la presente invención, preferiblemente

- se envía un mensaje de aceptación desde el servicio de protección de datos 200 al servicio de terceros 300, si el abonado permite el acceso del servicio de terceros 300 a los datos relacionados con el usuario a través del dispositivo informático 20, o
- se envía un mensaje de rechazo desde el servicio de protección de datos 200 al servicio de terceros 300, si el abonado rechaza el acceso del servicio de terceros 300 a los datos relacionados con el usuario a través del dispositivo informático 20.

En caso de que se use el método de identidad protegida, los datos relacionados con el usuario comprenden un identificador (ID), en donde el ID está relacionado con el abonado, en donde la relación entre el abonado y el ID es una relación de confianza existente (solo) dentro del servicio de protección de datos 200. Preferiblemente, el ID se proporciona al servicio de terceros 300 de manera fraudulenta, es decir, sin ninguna posibilidad para el servicio de terceros de conocer la verdadera identidad del abonado (identidad del usuario). Por ejemplo, el ID es una identidad digital generada aleatoriamente, que se genera, en particular, para cada sesión por separado. Preferiblemente, el ID es único para el abonado, una vez por sesión con el servicio de terceros 300 (ya que cambia cada vez).

En caso de que se use el sistema basado en permisos, no se proporcionan datos relacionados con el usuario al servicio de terceros 300. En cambio, se utiliza un sistema de concesión, en donde el abonado está habilitado para asignar al menos una información de autorización (por ejemplo, permisos) por servicio de terceros 300 y, en particular, por dato que el abonado desee utilizar para un servicio de terceros 300 seleccionado. Preferiblemente, el abonado está habilitado para permitir diferentes grados de niveles de privacidad o seguridad. Por ejemplo, se pueden compartir datos personales para servicios de pago, pero no para servicios de terceros 300 desconocidos.

Preferiblemente, cuando el abonado selecciona un primer nivel de seguridad, el servicio de protección de datos 200 protege (por ejemplo, excluye u oculta) - con respecto a los servicios de terceros 300 - al menos una primera información (y opcionalmente una segunda y/o una tercera información) de los datos de usuario y/o la identidad del usuario Preferiblemente, cuando el abonado selecciona el segundo nivel de seguridad, el servicio de protección de datos 200 protege al menos la segunda información (y opcionalmente la tercera información) de los datos de usuario y/o la identidad del usuario. Preferiblemente, cuando el usuario selecciona un tercer nivel de seguridad, el servicio de protección de datos 200 (solo) protege la tercera información de los datos de usuario y/o la identidad del usuario. Según un ejemplo, la primera información se refiere al menos a uno de detalles de la tarjeta de crédito, detalles de la cuenta bancaria, detalles del pasaporte, seguridad social y/u otros datos personales que un cliente rara vez divulga, salvo en un entorno de confianza. Según un ejemplo, la segunda información se refiere al menos a uno de fecha de nacimiento, inicio de sesión del correo electrónico, inicio de sesión de redes sociales y/u otros sitios/contraseñas útiles. Según un ejemplo, la tercera información se refiere a nombre, apellido, dirección, dirección de correo electrónico, estado civil, masculino/femenino, edad y/u otros detalles personales que el abonado generalmente divulga con frecuencia en los sitios web.

REIVINDICACIONES

1. Un método para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos (200),
en donde se accede al servicio de protección de datos (200) a través de una red de telecomunicaciones (100), por medio de un dispositivo informático (20) del abonado del servicio de protección de datos (200), el dispositivo informático (20) que se conecta a la red de telecomunicaciones (100),
en donde en caso de que el dispositivo informático (20) acceda a un servicio de terceros (300) a través de la red de telecomunicaciones (100), el servicio de terceros (300) recibe datos relacionados con el usuario, los datos relacionados con el usuario siendo datos relacionados con la identidad del usuario y/o los datos de usuario, en donde el acceso al servicio de terceros (300) a través del servicio de protección de datos (200) implica una transmisión de los datos relacionados con el usuario de modo que la identidad del usuario y/o los datos del usuario están al menos parcialmente protegidos y/o anonimizados con respecto al servicio de terceros (300)

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros (300), o
- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros (300) - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado,

caracterizado por que el servicio de protección de datos (200) crea un pasaporte digital dependiendo de la identidad del usuario y/o los datos de usuario del abonado, y además dependiendo de la información de autorización del abonado, en donde el abonado proporciona la información de autorización para el servicio de terceros (300).

2. El método según la reivindicación 1, en donde para una primera parte de la identidad del usuario y/o los datos de usuario, los datos relacionados con el usuario comprenden el texto plano de la identidad del usuario y/o los datos de usuario, y en donde para una segunda parte de la identidad del usuario y/o los datos de usuario, la transmisión al servicio de terceros (300) o bien se evita, o bien los datos relacionados con el usuario son datos modificados con respecto a la segunda parte de la identidad del usuario y/o los datos de usuario.

3. El método según la reivindicación 1, en donde la identidad del usuario y/o los datos de usuario están completamente protegidos y/o anonimizados con respecto al servicio de terceros (300)

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros (300), o
- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros (300) - siendo modificados con respecto a la identidad del usuario y/o los datos de usuario del abonado.

4. El método según una de las reivindicaciones anteriores, en donde la red de telecomunicaciones (100) es una red de comunicación móvil, y el dispositivo informático (20) es un dispositivo informático móvil, especialmente un teléfono móvil, un teléfono inteligente, una tableta, u otro dispositivo informático portátil.

5. El método según una de las reivindicaciones anteriores, en donde el servicio de terceros (300) es una aplicación proporcionada al dispositivo informático (20), en donde la aplicación se ejecuta en el dispositivo informático (20) o en un nodo de red de la red de telecomunicaciones (100), en donde al acceder al servicio de terceros (300) a través del servicio de protección de datos (200), el comportamiento de la aplicación se modifica con respecto a la transmisión de los datos relacionados con el usuario de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respecto al servicio de terceros (300).

6. El método según una de las reivindicaciones anteriores, en donde el método comprende anonimizar la identidad del usuario y los datos de usuario de modo que, al analizar los datos relacionados con el usuario transmitidos al servicio de terceros (300), la identidad del usuario asociada con el dispositivo informático (20) está oculta.

7. Un sistema para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos (200), el sistema que comprende el servicio de protección de datos (200), una red de telecomunicaciones (100) y un dispositivo informático (20),
en donde el sistema se configura de modo que se accede al servicio de protección de datos (200) a través de la red de telecomunicaciones (100), por medio del dispositivo informático (20) del abonado del servicio de protección de datos (200), el dispositivo informático (20) que se conecta a la red de telecomunicaciones (100),
en donde el sistema se configura de modo que en caso que el dispositivo informático (20) acceda a un servicio de terceros (300) a través de la red de telecomunicaciones (100), el servicio de terceros (300) recibe datos relacionados con el usuario, los datos relacionados con el usuario siendo datos relacionados con la identidad del usuario y/o datos de usuario, en donde el sistema se configura de modo que el acceso al servicio de terceros (300) a través del servicio de protección de datos (200) implica una transmisión de datos relacionados con el usuario de modo que la identidad del usuario y/o los datos de usuario están al menos parcialmente protegidos y/o anonimizados con respeto al servicio de terceros (300)

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros (300), o
- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros (300) - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado,

caracterizado por que el servicio de protección de datos (200) se configura para crear un pasaporte digital dependiendo de la identidad del usuario y/o los datos de usuario del abonado, y además dependiendo de la información de autorización del abonado, en donde el abonado proporciona la información de autorización para el servicio de terceros (300).

8. El sistema según la reivindicación 7, en donde el sistema se configura de modo que para una primera parte de la identidad del usuario y/o los datos de usuario, los datos relacionados con el usuario comprenden el texto plano de la identidad del usuario y/o los datos de usuario, y en donde el sistema se configura de modo que para una segunda parte de la identidad del usuario y/o los datos de usuario, la transmisión al servicio de terceros (300) o bien se evita, o bien los datos relacionados con el usuario son datos modificados con respecto a la segunda parte de la identidad del usuario y/o los datos de usuario.

9. El sistema según la reivindicación 7, en donde el sistema se configura de modo que la identidad del usuario y/o los datos de usuario están completamente protegidos y/o anonimizados con respecto al servicio de terceros (300)

- por medio de, al menos parcialmente, evitar la transmisión del texto plano de la identidad del usuario y/o los datos de usuario al servicio de terceros (300), o
- por medio de los datos relacionados con el usuario - transmitidos al servicio de terceros (300) - siendo modificados los datos con respecto a la identidad del usuario y/o los datos de usuario del abonado.

10. El sistema según una de las reivindicaciones 7 a 9, en donde la red de telecomunicaciones (100) es una red de comunicación móvil, y el dispositivo informático (20) es un dispositivo informático móvil, especialmente un teléfono móvil, un teléfono inteligente, una tableta, u otro dispositivo informático portátil.

11. Una red de comunicación móvil (100) adecuada para proteger y/o anonimizar una identidad de usuario y/o unos datos de usuario de un abonado de un servicio de protección de datos (200) en un sistema, según una de las reivindicaciones 7 a 10.

12. Un programa que comprende un código de programa legible por ordenador que, cuando se ejecuta en un ordenador o en un dispositivo informático (20) o en un componente de red de una red de telecomunicaciones (100) o en parte en un dispositivo informático (20) y en parte en un componente de red de una red de telecomunicaciones (100), hace que el ordenador o el dispositivo informático (20) y/o el componente de red de la red de telecomunicaciones (100) ejecuten un método según una de las reivindicaciones 1 a 6.

13. Un producto de programa de ordenador para usar un dispositivo de comunicación de tipo máquina (20) con una red de telecomunicaciones (100), el producto de programa de ordenador que comprende un programa de ordenador almacenado en un medio de almacenamiento, el programa de ordenador comprende el código de programa que, cuando se ejecuta en un ordenador o en un dispositivo informático (20) o en un componente de red de una red de telecomunicaciones (100) o en parte en un dispositivo informático (20) y en parte en un componente de red de una red de telecomunicaciones (100), hace que el ordenador o el dispositivo informático (20) y/o el componente de red de la red de telecomunicaciones (100) ejecuten un método según una de las reivindicaciones 1 a 6.

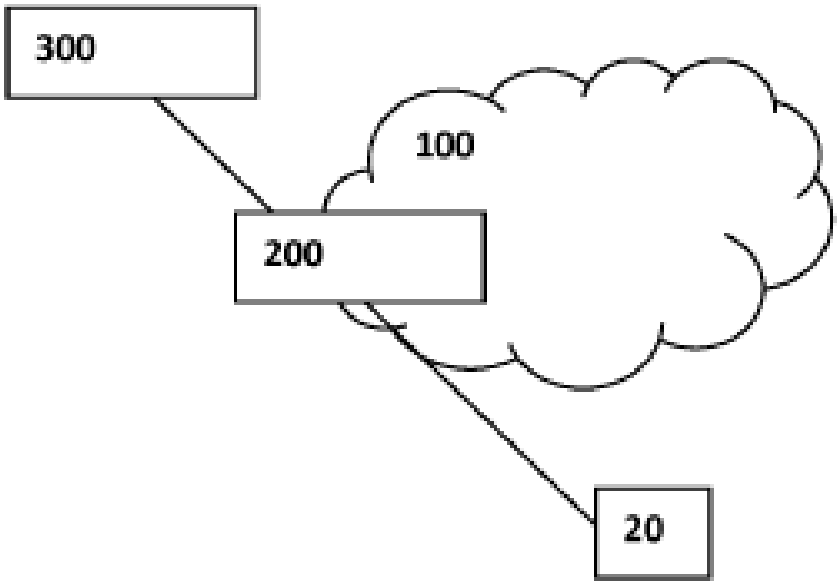


Fig. 1