(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 743 131**

(51) Int. CI.:

G06F 21/42 (2013.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.12.2012 PCT/FR2012/052953**

(87) Fecha y número de publicación internacional: **27.06.2013 WO13093314**

(96) Fecha de presentación y número de la solicitud europea: **17.12.2012 E 12812300 (7)**

(97) Fecha y número de publicación de la concesión europea: **26.06.2019 EP 2795870**

(54) Título: **Procedimiento de acceso por un terminal de telecomunicación a una base de datos alojada por una plataforma de servicios accesible mediante una red de telecomunicaciones**

(30) Prioridad:

23.12.2011 FR 1162439

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2020

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

LE HUEROU, EMMANUEL y
BEAUFILS, ERIC

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento de acceso por un terminal de telecomunicación a una base de datos alojada por una plataforma de servicios accesible mediante una red de telecomunicaciones

La invención se refiere, de manera general, al campo de las telecomunicaciones y, más precisamente, al acceso por diversos terminales de telecomunicaciones a unos datos almacenados por un servidor en una red de telecomunicaciones.

La presente invención se aplica, en concreto, a un sistema llamado "de informática en la nube" (de la expresión inglesa "*cloud computing*"), es decir, un sistema informático que permite a los particulares almacenar sus datos personales en unos servidores, pero, igualmente, a las empresas que no disponen de sus propios servidores almacenar sus datos en unos servidores que alquilan; de este modo, estas últimas delegan sus operaciones de cálculo y de almacenamiento a unos proveedores de servicios que se benefician de infraestructuras informáticas dispersas en todo el mundo y unidas entre sí por una red. El acceso a esta "informática en la nube" se hace generalmente *mediante* Internet y, en este contexto, un usuario particular o de empresa accede a sus aplicaciones y sus datos alojados en un servidor remoto a través de una "oficina virtual", *mediante* cualquier terminal conectado a la red.

De este modo, de manera general, el usuario se conecta a un servidor o plataforma de servicios en la que se aloja una base de datos que contiene sus datos personales - por ejemplo, unas fotos, unos vídeos, unos documentos, etc. - desde un terminal informático, tal como un ordenador personal, en el que se descarga una página web de acceso a un portal de entrada de la plataforma de servicios o bien a partir de una aplicación de software previamente instalada en el terminal informático considerado. A título de ejemplos, unos servicios de almacenamiento de datos informáticos de este tipo en "la nube" son ofrecidos por unas compañías, tales como Dropbox *(Dropbox™,* almacenamiento y compartición de archivos en línea) o Google *(Picasa Web Album™,* gestión de fotos en la web).

Para conectarse a su espacio personal en la red, de manera convencional, el usuario ingresa un identificador de usuario *(login)* y una contraseña *(password)* a partir de su terminal conectado a una red de tipo IP *(Internet Protocol, Protocolo de Internet).* Después de verificación de su identidad por el servidor, el usuario accede a su entorno de datos personales. De este modo, el usuario puede conectarse a su entorno de datos personales alojado por la plataforma de servicios desde diversos terminales informáticos conectados a internet de manera fija (ordenador personal, por ejemplo) o en movilidad (teléfono inteligente o *smartphone*, tableta digital, ...).

En este contexto, cada vez que quiera cambiar de terminal informático para conectarse a su espacio personal, el usuario deberá volver a comenzar desde el nuevo terminal la tramitación de conexión con identificador y contraseña. Por otra parte, si el usuario citado anteriormente quiere dar acceso a su entorno de datos a un usuario tercero remoto, provisto de su propio terminal, deberá comunicar a este usuario tercero sus datos personales de identificación.

La presente invención tiene como objetivo mejorar la situación expuesta más arriba permitiendo, en concreto, que un usuario use cualquier terminal conectado a Internet para acceder a unos datos personales almacenados en la "nube" en unas condiciones de seguridad y de comodidad de uso mejoradas.

La presente invención se define por una primera reivindicación independiente de procedimiento (reivindicación 1), una segunda reivindicación independiente de terminal (reivindicación 10), una tercera reivindicación independiente de servidor (reivindicación 13) y una cuarta reivindicación independiente de módulo de software (reivindicación 15) que se refiere a un acceso fácil y seguro a unos datos almacenados en una red de comunicaciones.

Para tal fin, según un primer aspecto, la presente invención se refiere a un procedimiento de acceso por un primer terminal de telecomunicación a una base de datos alojada por una plataforma de servicios accesible mediante una red de telecomunicaciones. De conformidad con la invención, este procedimiento incluye, de manera general:

(A) - la transmisión de una información representativa de una petición de acceso del primer terminal a la base de datos, con destino a un segundo terminal asociado a un identificador de abonado a una segunda red de telecomunicaciones, correspondiendo dicho identificador de abonado al segundo terminal;
(B) - en el segundo terminal, el envío de una respuesta a la petición de acceso con destino a un servidor de autenticación de la plataforma, comprendiendo dicha respuesta un identificador del primer terminal (T1) y el identificador de abonado del segundo terminal (T2);
(C) - en el servidor de autenticación, cuando se recibe una respuesta a la petición de acceso, la verificación del identificador del abonado a la segunda red y la validación o no del acceso a la base de datos por el primer terminal en función del resultado de la verificación citada anteriormente.

Según el procedimiento de la invención, definido más arriba en términos generales, el acceso del primer terminal a la base de datos de la plataforma de servicios está condicionado por la autorización recibida que proviene de un segundo terminal de telecomunicaciones, por ejemplo, un *teléfono inteligente,* cuyo identificador de abonado - en la práctica, el número de teléfono (número MSISDN) almacenado en la tarjeta SIM del teléfono, cuando este segundo teléfono es un terminal de telefonía móvil -, es autenticado por el servidor de autenticación.

En la práctica, cuando el segundo terminal es un teléfono móvil, el usuario del segundo terminal propietario de los datos personales almacenados en la red, puede, de este modo, autorizar rápida y simplemente el acceso a sus datos personales a otro terminal con su teléfono móvil. En efecto, el número MSISDN *(Mobile Station ISDN Number, Número RDSI de la Estación Móvil)* almacenado en la tarjeta SIM *(Subscriber Identity Module, Módulo de Identidad del Suscriptor)* del teléfono móvil es deducible de la respuesta a la petición de acceso, luego, es autenticado en el servidor, lo que permite garantizar de manera fiable el origen de la respuesta a la petición de acceso.

Según un modo de realización particular de la invención, los primer y segundo terminales de telecomunicación están conectados a la misma red de comunicación. En este caso, la red de comunicación de acceso a la plataforma de servicio y la segunda red de comunicación citada anteriormente son una misma y única red. Por ejemplo, los primer y segundo terminales pueden ser ambos dos unos terminales móviles conectados a la misma red de telefonía móvil.

Según un primer modo de realización de la invención, la etapa (A) del procedimiento citado anteriormente comprende:

(a1) - en el primer terminal de telecomunicación, generación de una petición de acceso a la base de datos, constando la petición de una información de identificación del abonado a la segunda red de telecomunicaciones y envío de la petición de acceso al servidor de autenticación de la plataforma;
(a2) - en el servidor de autenticación, determinación del segundo terminal de telecomunicación a partir de la información de identificación de abonado extraída de la petición de acceso recibida, luego, transmisión al segundo terminal de una solicitud de autorización de acceso del primer terminal a la base de datos.

En este modo de realización, es el servidor de autenticación el que determina el segundo terminal (el terminal móvil) a partir de la información de identificación de abonado. Según una característica particular de este modo de realización, la etapa (A) consta de una operación previa de carga y de visualización en el primer terminal de una página web de acceso al servidor de autenticación de la plataforma de servicios, siguiendo la petición de acceso al servidor de autenticación a un comando del usuario del primer terminal transmitido mediante dicha página web.

Por ejemplo, el comando del usuario del primer terminal puede ser simplemente la introducción en el teclado del primer terminal, del número de teléfono del usuario del segundo terminal. Por lo tanto, no es necesario que el primer usuario introduzca un identificador y una contraseña como es este el caso en la mayor parte de las aplicaciones conocidas del estado de la técnica.

Según otra característica de la invención, la etapa (B) mencionada anteriormente del procedimiento de acceso según la invención comprende:

(b1) - notificación de la solicitud de autorización de acceso en el segundo terminal; y
(b2) - como continuación a una acción de un usuario del segundo terminal efectuada por medio de una interfaz hombre-máquina del segundo terminal, envío de una respuesta a la solicitud de autorización de acceso con destino al servidor de autenticación.

De este modo, como se ha expuesto más arriba, en este primer modo de realización, es el servidor de autenticación el que actúa como intermediario entre el usuario del primer terminal y el del segundo terminal, propietario de los datos a los que el primer usuario quiere acceder. Este modo de realización está, de este modo, particularmente adaptado para la situación en la que los primer y segundo usuarios son remotos uno del otro. En este contexto, el acceso a la base de datos por el primer terminal permite, por ejemplo, realizar una aplicación de compartición de datos de la base de datos, cuya implementación es validada por el usuario del segundo terminal a solicitud del usuario del primer terminal.

Según una característica de realización, siempre en el modo de realización expuesto más arriba, el procedimiento según la invención comprende la visualización en el segundo terminal de una interfaz gráfica que visualiza unas informaciones relativas a las solicitudes de acceso y al estado de conexión con la plataforma de servicios para un conjunto de terminales de telecomunicaciones predeterminado.

Gracias a esta disposición, el usuario del segundo terminal dispone de un medio eficiente y simple de usar para suministrar, luego, controlar el acceso, por unos usuarios terceros, a unos datos de su espacio de datos personales en la plataforma de servicios.

Según un modo de realización particular, para un conjunto predeterminado de primeros terminales identificados en una lista almacenada en el segundo terminal, el segundo terminal envía automáticamente una respuesta a la petición de acceso recibida con destino al servidor de autenticación. Por ejemplo, esta respuesta se podrá enviar automáticamente después de una duración predeterminada (temporización) sin intervención del usuario.

De este modo, el segundo terminal transmite automáticamente una respuesta al servidor de autenticación sin intervención del usuario del segundo terminal, para un terminal considerado de la lista. Por ejemplo, si el segundo terminal es un teléfono móvil y el primer terminal una tableta digital que pertenece a un mismo usuario, este último

queda, de este modo, exento de la etapa de validación por envío de una respuesta al servidor de autenticación, cuando la tableta se identifica en la lista.

Según una variante de realización, la lista citada anteriormente de primeros terminales está almacenada en el servidor de autenticación, la etapa (a2) de transmisión al segundo terminal de una solicitud de autorización de acceso del primer terminal a la base de datos no se implementa, entonces, cuando el primer terminal se identifica como que es un terminal de la lista, siendo el acceso del primer terminal a la base de datos validado automáticamente por el servidor de autenticación.

Según un segundo modo de realización del procedimiento de la invención, que puede combinarse ventajosamente con el primer modo de realización expuesto más arriba, el procedimiento comprende una operación previa de carga y de visualización en el primer terminal de una página web de acceso al servidor de autenticación de la plataforma y en el que la página web de acceso al servidor de autenticación de la plataforma de servicios, visualizada en una pantalla del primer terminal, representa un código de dos dimensiones generado automáticamente por el servidor de autenticación durante la descarga de la página web; la etapa (A) de transmisión de una información representativa de una petición de acceso a la base de datos del primer terminal al segundo terminal, consiste, entonces, en transmitir este código de dos dimensiones a una aplicación de software instalada en el segundo terminal.

En particular, en este modo de realización, en la etapa (B), la respuesta a la petición de acceso enviada del segundo terminal con destino al servidor de autenticación consta del código de dos dimensiones citado anteriormente. El servidor de autenticación compara, entonces, el código recibido con el código generado inicialmente.

Según un modo de realización preferido, la segunda red de telecomunicaciones es una red de telefonía móvil y el segundo terminal es un teléfono móvil de tipo *teléfono inteligente.*

En este segundo modo de realización, la transmisión de la petición de acceso tiene lugar directamente del primer terminal hacia el segundo terminal, por ejemplo, por fotografía por el segundo terminal del código visualizado en la pantalla del primer terminal. Se comprenderá, entonces, que este modo de realización está particularmente adaptado para la situación en la que los dos terminales están situados en la proximidad uno del otro, por ejemplo, en la misma habitación. En este contexto, el acceso a la base de datos por el primer terminal permite, por ejemplo, realizar una aplicación de desvío de visualización de datos, del segundo terminal hacia el primer terminal, en el caso, por ejemplo, donde este último disponga de capacidades de visualización más amplias que las del segundo terminal. Por supuesto, según este segundo modo de realización, el usuario del primer terminal y el del segundo terminal pueden ser las mismas personas.

Según un segundo aspecto, la presente invención tiene como objeto un terminal de telecomunicación que comprende:

- unos medios de recepción de una información representativa de una petición de acceso de un primer terminal de telecomunicación a una base de datos alojada por una plataforma de servicios en una red de telecomunicaciones;
- unos medios de generación y de envío de una respuesta a la petición de acceso con destino a un servidor de autenticación de la plataforma de servicios, con el fin de verificar un identificador de abonado a una segunda red de telecomunicaciones, correspondiendo dicho identificador de abonado al segundo terminal, al que está conectado dicho terminal de telecomunicación, comprendiendo dicha respuesta un identificador del primer terminal (T1) y el identificador de abonado del segundo terminal (T2) y de validar el acceso a la base de datos por el primer terminal en función del resultado de la verificación del identificador de abonado.

Según una característica particular, un terminal de telecomunicaciones de este tipo según la invención incluye, además, unos medios de interfaz hombre-máquina adaptados para notificar a un usuario del terminal la información citada anteriormente representativa de la petición de acceso y para enviar una respuesta a la petición de acceso con destino a un servidor de autenticación, como continuación a una acción del usuario efectuada mediante la interfaz hombre-máquina.

Según otra característica de un terminal de telecomunicaciones de este tipo, este incluye unos medios de interfaz gráfica adaptados para visualizar unas informaciones relativas a las peticiones de acceso y al estado de conexión con la plataforma de servicios para un conjunto de terminales de telecomunicaciones predefinido.

De este modo, el usuario de un (segundo) terminal según la invención, "propietario" de los datos, podrá conservar ventajosamente el control de las conexiones en curso con la base de datos para un conjunto predefinido de terminales de usuarios. En particular, el usuario del terminal según la invención tendrá, mediante la interfaz gráfica, la posibilidad de interrumpir una conexión en curso entre un primer terminal de entre el conjunto de terminales predefinido y la base de datos.

Según un modo particular de realización, un terminal de telecomunicación de este tipo incluye unos medios de recepción y de lectura de un código de dos dimensiones transmitido por el primer terminal, siendo este código representativo de una petición de acceso a la base de datos por el primer terminal. En este modo de realización, la respuesta a la petición de acceso con destino a un servidor de autenticación consta del código de dos dimensiones.

Según un tercer aspecto, la presente invención tiene como objeto un servidor de autenticación para la implementación de un procedimiento de acceso a una base de datos, tal como se ha expuesto brevemente más arriba, comprendiendo este servidor:

- unos medios de recepción de una respuesta a una petición de acceso de un primer terminal de telecomunicación a la base de datos, que proviene de un segundo terminal de telefonía móvil según la invención, comprendiendo dicha respuesta un identificador del primer terminal (T1) y un identificador de abonado del segundo terminal (T2); y
- unos medios de verificación del identificador de abonado a una red de telefonía móvil que corresponde al segundo terminal como continuación a la recepción de la respuesta a una petición de acceso y de validación del acceso a la base de datos por el primer terminal en función del resultado de dicha verificación.

Se comprenderá que un servidor de este tipo está particularmente adaptado para un procedimiento de acceso a una base de datos, tal como se ha expuesto brevemente más arriba en el contexto del primer modo de realización.

Además, un servidor de este tipo según la invención incluye:

- unos medios de recepción de una petición de acceso a la base de datos que proviene del primer terminal, contando la petición de una información de identificación de un abonado a una red de telefonía móvil;
- unos medios de determinación de un segundo terminal de telecomunicación a partir de la información de identificación de abonado extraída de la petición de acceso recibida; y,
- unos medios de transmisión al segundo terminal de una solicitud de autorización de acceso del primer terminal a la base de datos.

Finalmente, según un último aspecto, la invención tiene como objeto un módulo de software destinado a estar incorporado en un terminal de telecomunicaciones según la invención, tal como se ha expuesto brevemente más arriba o bien destinado a estar incorporado en un servidor de autenticación según la invención, tal como se ha expuesto brevemente más arriba. Un módulo de software de este tipo incluye unas instrucciones de programa cuya ejecución por un procesador informático permite implementar las etapas de un procedimiento de acceso a una base de datos, según la invención, que se ejecutan, según el caso considerado, en un terminal de telecomunicaciones según la invención o bien en un servidor de autenticación según la invención.

Por otra parte, un módulo de software de este tipo puede usar cualquier lenguaje de programación y comprender unos programas en forma de código fuente, código objeto o de código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

Por consiguiente, la invención también tiene como objetivo un soporte de grabación de informaciones legible por un ordenador y que incluye unas instrucciones de programa de ordenador. Un soporte de grabación de este tipo puede estar constituido por cualquier entidad o dispositivo capaz de almacenar un programa de este tipo. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo, un CD ROM o una ROM de circuito microelectrónico o también un medio de grabación amovible, tal como una llave USB o un medio de grabación magnético, tal como un disco duro. Por otra parte, un módulo de software según la invención puede descargarse, en particular, en una red de tipo Internet.

Las ventajas que procura un terminal de telecomunicaciones, un servidor de autenticación, un módulo de software, tales como se han definido brevemente más arriba, son idénticas o contribuyen a las mencionadas más arriba en relación con el procedimiento de acceso a una base de datos, según la invención y, por consiguiente, no se recordarán, en el presente documento.

Otras características y ventajas de la presente invención se desprenderán de la descripción detallada que sigue, que hace referencia a los dibujos adjuntos en los que:

- la figura 1 ilustra un sistema de telecomunicaciones en el que se implementa la invención y, en particular, ilustra los elementos funcionales incorporados respectivamente en un terminal de telecomunicación y en un servidor de autenticación, según la invención;
- la figura 2 representa en forma de diagrama de flujo las principales etapas de un procedimiento de acceso por un terminal de telecomunicaciones a una base de datos alojada por una plataforma de servicios, según la invención; y
- la figura 3 ilustra un ejemplo de intercambios de mensajes entre los diferentes elementos del sistema de telecomunicaciones de la figura 1, para la implementación de un procedimiento de acceso a una base de datos, según la invención.

La figura 1 ilustra un sistema de telecomunicaciones en el que se implementa la invención. Como se representa en la figura 1, un primer terminal de telecomunicación T1 está conectado a la red de telecomunicaciones RED constituida, en el presente documento, por una red IP de tipo Internet. El terminal T1 en este ejemplo de realización es ordenador

personal, pero puede tratarse de una tableta digital o táctil o también de un *teléfono inteligente* conectado a Internet.

El sistema también comprende una plataforma de servicios PTF conectada a la red RED y que ofrece diversos servicios, tales como el almacenamiento de datos personales "en la nube" *(cloud storage)* - por ejemplo, unos documentos multimedia, tales como unos vídeos, fotos, unos documentos de texto, etc. La plataforma de servicios PTF comprende un servidor de autenticación AUT asociado a una base de datos BD de usuarios de los servicios y un servidor SVR de datos que almacena los datos personales de los usuarios inscritos en el servicio de almacenamiento de datos personales.

La base de datos de usuarios (BD), asociada al servidor de autenticación, contiene para cada usuario de la plataforma de servicios, una lista o una tabla memorizada que contiene un identificador de usuario o abonado al servicio de almacenamiento de datos - por ejemplo, un nombre de usuario - asociado a al menos un identificador de abonado a una red de telefonía o un identificador de terminal, por ejemplo, un número de teléfono móvil, un número de teléfono IP fijo, una dirección IP. Además, una tabla de usuario de este tipo puede comprender ventajosamente otro identificador de comunicación, tal como una dirección de correo electrónico. De este modo, el usuario de un terminal T1, podrá usar una dirección de correo electrónico como identificador de usuario para permitir que el servidor de autenticación identifique a un usuario inscrito en la base de datos de usuarios (BD) y determinar, a continuación, un terminal (T2) asociado al usuario identificado.

El sistema representado comprende, igualmente, un segundo terminal de telecomunicación, T2, conectado a la red RED. En el ejemplo de realización descrito e ilustrado, el terminal T2 es un terminal de telefonía móvil de tipo *teléfono inteligente.* El teléfono móvil T2 está representado en la figura 1 conectado a la red RED para simplificar la exposición. Sin embargo, el terminal T2 puede estar unido, en la práctica, a la red RED a través de una red de acceso, por ejemplo, una red WiFi o bien a través de una red móvil de tercera generación (UMTS) (conexión en modo *datos).*

Como se representa en la figura 1, el terminal móvil T2 consta, en concreto, de los siguientes módulos funcionales:

- Un módulo de comunicación de entrada/salida, anotado "E/S" y destinado a comunicar con la red RED.
- Un módulo sistema operativo, SO2, por ejemplo, el sistema operativo Android™ de la compañía Google, que gestiona la interacción entre los diferentes módulos y el procesador (no representado) del terminal T2.
- Un dispositivo de visualización asociado a un teclado (táctil o mecánico) "PANT/TECL".
- Un módulo memoria MEM2 en el que está almacenada una aplicación o módulo de software APLI2 según la invención.

El módulo E/S permite, en particular, recibir una información representativa de una petición de acceso del primer terminal de telecomunicación T1 a los datos personales del usuario del terminal T2 almacenados en el servidor SVR de la plataforma de servicios PTF, luego, comunicar esta información a la aplicación APLI2.

La aplicación APLI2 consta de unas instrucciones de programa adaptadas para generar una respuesta a la petición de acceso, transmitida, a continuación, al módulo E/S que, a su vez, la transmite con destino al servidor de autenticación AUT, a través de la red RED.

La aplicación APLI2 del terminal T2 también consta de unas instrucciones cuya ejecución produce una interfaz hombre-máquina - en la práctica, una interfaz gráfica visualizada por la pantalla PANT del terminal -, mediante la que el usuario del terminal T2 recibe notificación de una información representativa de la petición de acceso y le permite enviar una respuesta a la petición de acceso con destino al servidor de autenticación.

En el modo de realización presentado, la interfaz gráfica producida por la aplicación APLI2 está adaptada para visualizar unas informaciones relativas a las peticiones de acceso y al estado de conexión con la plataforma de servicios PTF para un conjunto de terminales de telecomunicaciones predeterminado. Este conjunto de terminales puede constar de otros terminales del usuario principal del terminal T2 (un terminal móvil en el modo de realización ilustrado), como, por ejemplo, una tableta digital o un ordenador personal doméstico o bien unos terminales de telecomunicaciones que pertenecen a unas personas elegidas por el usuario del terminal T2 (por ejemplo, unos amigos o unas personas de su familia).

Según un modo particular de realización, el terminal T2 comprende, además, un módulo de lectura de un código de dos dimensiones, integrado o asociado a la aplicación APLI2 y que permite, en concreto, leer un código de dos dimensiones transmitido por el primer terminal T1, código que es representativo de una petición de acceso a la base de datos por el terminal T1.

En este modo de realización, una respuesta a una petición de acceso transmitida por el terminal T2 con destino al servidor de autenticación consta de un código de dos dimensiones de este tipo, comprando el servidor de autenticación, a continuación, el código recibido con el código generado inicialmente. En la práctica, un código de dos dimensiones de este tipo puede estar constituido por un código de barra de dos dimensiones, tal como un código QR.

Según una variante de realización, un terminal T2 según la invención puede estar equipado con un lector de etiqueta

(tag en inglés) NFC destinado a leer una etiqueta NFC *(Near Field Communication*, *Comunicación de Campo Cercano)* que equipa y programada por el terminal T1.

Siempre en la figura 1, el servidor de autenticación AUT de la plataforma de servicios PTF incluye correlativamente los siguientes módulos funcionales:

- Un módulo de comunicación de entrada/salida, anotado "E/S-A" y destinado a comunicar con la red RED y recibir una petición de acceso a la base de datos que proviene del primer terminal T1, constando esta petición de acceso de una información de identificación de un usuario inscrito en los servicios proporcionados por la plataforma de servicios PTF. En el modo de realización descrito, esta información de identificación de usuario es una información de identificación de un abonado a una segunda red de telecomunicaciones - en el presente documento, una red de telefonía móvil, siendo la información de identificación, por ejemplo, el número de teléfono asociado a la tarjeta SIM incorporada en el terminal T2. El módulo E/S-A está encargado, igualmente, de transmitir al segundo terminal T2, identificado gracias a la información de identificación citada anteriormente, una solicitud de autorización de acceso del primer terminal T1.
- Un módulo sistema operativo, SO-A, que gestiona la interacción entre los diferentes módulos y el procesador (no representado) del servidor.
- Un módulo memoria MEM-A en el que está almacenada una aplicación o módulo de software APLI-A según la invención, cuyas instrucciones de programa, cuando son ejecutadas por un procesador (no representado) del servidor AUT, permiten implementar las etapas del procedimiento de acceso según la invención que se implementan en el servidor de autenticación. En particular, el módulo de software APLI-A está diseñado para verificar un identificador de un segundo terminal T2, - es decir, en el modo de realización descrito, un identificador de abonado (número de teléfono) de una red de telefonía móvil -, como continuación a la recepción de una respuesta a una petición de acceso, que proviene del terminal T2; y, por otra parte, para validar o no el acceso a la base de datos (SVR) por el primer terminal T1 en función del resultado de la verificación citada anteriormente.

La figura 2 representa en forma de diagrama de flujo las principales etapas del procedimiento de acceso por un terminal de telecomunicaciones T1 a una base de datos SVR alojada por una plataforma de servicios PTF.

Como se representa en la figura 2, el procedimiento según la invención comienza por la etapa E10 durante la que el terminal T1, conectado a la red de Internet, carga una página web de acceso al servidor de autenticación AUT de la plataforma de servicios, por ejemplo, una dirección del tipo "*cloudphone.orange.fr*". El usuario del terminal T1 conoce al menos un identificador de comunicación que permite identificar al propietario de los datos que desea consultar, por ejemplo, un álbum de fotos. Este identificador de comunicación puede ser una dirección de correo electrónico, un número de teléfono fijo, un número de teléfono móvil o bien un nombre de persona.

El usuario del terminal T1 introduce en la pantalla del terminal este identificador, en un campo dedicado de la página web. Supongamos que este identificador sea una dirección de correo electrónico, entonces, se genera una petición de acceso a los datos, esta consta de la información de identificación constituida por la dirección de correo electrónico del propietario de los datos. La petición de acceso se envía, entonces, al servidor de autenticación AUT.

En la etapa E12 que sigue, el servidor de autenticación recibe la petición de acceso que proviene del terminal T1, extrae la información de identificación de una persona, en este ejemplo, una dirección de correo electrónico y consulta la base de datos de usuarios BD con esta dirección de correo electrónico como parámetro de entrada, para obtener al menos un identificador de abonado a una red de comunicaciones. En este ejemplo, el servidor AUT obtiene un número de teléfono móvil. El servidor de autenticación transmite, entonces, al terminal móvil T2 que corresponde al número de teléfono móvil obtenido, una solicitud de autorización de acceso representativa de la petición de acceso del primer terminal a los datos personales de la persona identificada por el número de teléfono móvil citado anteriormente, en la base de datos de usuarios BD de la plataforma de servicios PTF.

En la siguiente etapa, E14, en el terminal móvil T2, se recibe la solicitud de autorización de acceso por la aplicación APLI2 y se notifica al usuario del terminal, por ejemplo, por un tono de llamada específico. Según unas variantes de realización, la notificación al terminal T2 de la solicitud de autorización de acceso se puede efectuar por el envío de un mensaje de tipo SMS o MMS o bien por una llamada telefónica disparada automáticamente por un servidor de voz interactivo activado con comando por el servidor de autenticación. Una vez que la solicitud de autorización de acceso ha sido notificada al usuario del segundo terminal, este puede disparar, entonces, mediante la interfaz gráfica visualizada por la aplicación APLI2 del terminal T2, el envío de una respuesta a la solicitud de autorización de acceso, con destino al servidor de autenticación AUT.

Como se ha expuesto más arriba en la descripción, según un modo de realización ventajoso de la invención, el propietario de los datos que hay que compartir y usuario del terminal T2 tiene la posibilidad de predefinir una lista de terminales T1, almacenada en el terminal T2 o accesible en la red por la aplicación APLI2 del terminal T2, para los que el segundo terminal envía automáticamente una respuesta favorable a la petición de acceso recibida con destino al servidor de autenticación. Según una variante de realización que se puede combinar con la anterior, una lista predefinida de terminales de este tipo puede estar almacenada en el servidor de autenticación, en este caso, la etapa de transmisión al terminal T2 de una solicitud de autorización de acceso no se implementa para los terminales

identificados en la lista citada anteriormente.

En la etapa E16, cuando el servidor de autenticación AUT recibe una respuesta a la solicitud de autorización que proviene del terminal T2, analiza la respuesta y valida o no el acceso a la base de datos por el primer terminal en función del contenido de la respuesta.

Si el acceso es validado, se establece una sesión de consulta de datos entre el terminal T1 y el servidor de datos SVR. La aplicación APLI2 del segundo terminal T2 visualiza una interfaz gráfica que presenta el estado de la sesión de consulta entre el terminal T1 y el servidor de datos SVR y el usuario del terminal T2 tiene la posibilidad, de este modo, de controlar la sesión en curso.

En el segundo modo de realización presentado más arriba en la descripción, en el terminal T1, la página web de acceso al servidor de autenticación de la plataforma de servicios provoca la visualización de un código de dos dimensiones generado automáticamente por el servidor de autenticación durante la descarga de la página web. Por consiguiente, la etapa E12 de la figura 2 está "cortocircuitada", ya que el código de dos dimensiones se transmite directamente del primer terminal T1 al segundo terminal T2, por ejemplo, por fotografía del código por el terminal T2. En este caso, la respuesta a la solicitud de autorización de acceso, generada por el terminal T2 en la etapa E14, consta del código fotografiado.

En la práctica, en los modos de realización expuestos, en el presente documento, los intercambios entre los terminales T1 y T2 y el servidor AUT se implementan por unos comandos que usan el lenguaje XML conocido *(Extensible Markup Language, Lenguaje de Marcado Extensible)* y se transmiten según el protocolo de comunicación HTTP conocido *(HyperText Transfer Protocol, Protocolo de Transferencia de Hipertexto).*

La figura 3 ilustra un ejemplo de intercambios de mensajes entre los diferentes elementos del sistema de telecomunicaciones de la figura 1, para la implementación de un procedimiento de acceso a una base de datos, según los primer y segundo modos de realización de la invención. En la figura 3, las referencias "T1-U1", "T2-U2" y AUT y las líneas verticales correspondientes, indican las acciones implementadas respectivamente en el terminal T1 cuyo usuario es U1, el terminal T2 cuyo usuario es U2 y en el servidor de autenticación AUT. La figura 3 ilustra, de este modo, un ejemplo de proceso de acceso por un usuario U1 del terminal T1 a unos datos personales, almacenados en la plataforma de servicios (PTF), de un usuario U2 del terminal T2.

El proceso comienza por el envío de un mensaje m1 del terminal T1 hacia el servidor AUT, este mensaje m1 contiene una petición de un código secreto del terminal T1 hacia el servidor AUT, de la forma *getSecret(T1) (obtenerSecreto(T1)),* por ejemplo. A cambio, el servidor AUT transmite al terminal T1 un mensaje m2 que contiene un código secreto generado de manera aleatoria en el servidor. El mensaje m2 contiene un comando, por ejemplo, de la forma *setSecret(secret)* (*ajustarSecreto(secreto)* donde *secret*o es el código secreto. El intercambio previo de un código secreto entre el servidor AUT y el terminal T1 permite, de este modo, asegurar más el procedimiento de acceso según la invención.

A continuación, como se representa en E30, habiendo el terminal T1 recibido el código secreto, este último se visualiza en el terminal T1 y paralelamente, un elemento, legible por un dispositivo exterior, que contiene el código secreto y un identificador del terminal T1 (por ejemplo, su dirección IP), se produce en el terminal T1. Este elemento "legible" es, por ejemplo, un código de barra, tal como un *Código QR* o etiqueta NFC. Entonces, hay que considerar dos casos, el caso "M1" que corresponde al primer modo de realización expuesto más arriba o el caso "M2" que corresponde al segundo modo de realización expuesto más arriba.

Según el primer modo de realización (M1), el usuario U1 del primer terminal T1 dispara, mediante la página web de acceso al servidor AUT, la transmisión de un mensaje m3 que contiene la petición de acceso a los datos, con destino al servidor AUT, constando la petición de acceso de un identificador del usuario U2 (por ejemplo, un número de teléfono móvil). El mensaje m3 contiene un comando, por ejemplo, de la forma *getAccess(T1, U2, secret) (obtenerAcceso(T1, U2, secreto).*

Como continuación a la recepción del mensaje m3, el servidor AUT determina el terminal T2 y le envía un mensaje m4 que contiene una solicitud de autorización de acceso del terminal T1 a unos datos personales del usuario U1. Este mensaje m4 contiene un comando, por ejemplo, de la forma *getAccess(T1, secret) (obtenerAcceso(T1, secreto).*

Como continuación a la recepción del mensaje m4 en el terminal T2, según el ejemplo de intercambios expuesto, como se representa por el recuadro E32, habiendo el usuario U2 recibido el código *secreto* (por ejemplo, un código de cuatro cifras) se pone en contacto con el usuario U1 para verificar que el usuario U1 está en posesión del código secreto y que, por consiguiente, la petición de acceso que proviene del terminal T1 es correctamente auténtica. Esta puesta en contacto del usuario U2 con el usuario U1 se puede realizar por comunicación de voz, por ejemplo, cuando los terminales T1 y T2 son geográficamente remotos uno del otro o bien por una comunicación oral cuando los terminales están cerca uno del otro (en una misma habitación, por ejemplo) y los usuarios U1 y U2 son distintos.

La operación opcional de más arriba de verificación del código secreto permite garantizar, en concreto, que la petición

de acceso no ha sido enviada por un pirata informático que haya usurpado la identidad del terminal T1.

Si el terminal T1 se ha autenticado correctamente por el usuario T1, el usuario U1 dispara en el terminal T1 el envío con destino al servidor AUT de un mensaje m5 que contiene una respuesta favorable a la solicitud de autorización contenida en el mensaje m4, por ejemplo, un comando de la forma *setAutorisation(T1, U2, secret) (ajustarAutorización(T1, U2, secreto).*

Como respuesta, el servidor AUT envía un mensaje m6 al terminal T1, conteniendo el mensaje m6 una clave digital de autorización que permite al terminal T1 desbloquear el acceso a los datos que el usuario U1 desea consultar y que están almacenados en el servidor de datos SVR de la plataforma de servicios PTF. El mensaje m6 contiene un comando que es, por ejemplo, de la forma *setAutorisation(autorisationKey) (ajustarAutorización(autorizaciónClave).* Habiendo el terminal T1 recibido la clave de autorización o testigo *(token* en inglés), el acceso por el terminal T1 a los datos del usuario U2 está, desde ese momento, autorizado (recuadro E34) con la condición de la presentación por el terminal T1 del testigo al servidor de autenticación AUT; el usuario U1 podrá consultar, entonces, los datos personales del usuario U2.

Siempre en la figura 3, según el segundo modo de realización (M2) de la invención, expuesto más arriba, como continuación a la descarga de la página web de acceso a la plataforma de servicios, un elemento legible que contiene el código secreto y el identificador del terminal T1 se produce en el terminal T1 en la forma, por ejemplo, de un código de barras o de una etiqueta *(tag)* NFC programada en el terminal T1. En este modo de realización, encontrándose el terminal T2 en la proximidad del terminal T1 y disponiendo de un dispositivo de lectura adaptado, lee el código secreto proporcionado por el terminal T1 (representado por la flecha m7). Como continuación a la lectura del código secreto, la aplicación informática APLI2, según la invención, que equipa el terminal T2, transmite, entonces, automáticamente al servidor de autenticación AUT el mensaje m8, que contiene una respuesta favorable a la solicitud de autorización obtenida por lectura (flecha m7) por el terminal T2 del elemento "legible" citado anteriormente, producido en el terminal T1. El mensaje m8 contiene un comando de la forma, por ejemplo, *setAutorisation(T1, U2, secret) (ajustarAutorización(T1, U2, secreto).*

Finalmente, al igual que para el primer modo de funcionamiento, como respuesta al mensaje m8, el servidor AUT envía un mensaje m9 al terminal T1, conteniendo el mensaje m9 una clave digital de autorización que permite al terminal T1 desbloquear el acceso a los datos que el usuario U1 desea consultar y que están almacenados en el servidor de datos SVR de la plataforma de servicios PTF. El mensaje m9 contiene un comando, por ejemplo, de la forma *setAutorisation(autorisationKey) (ajustarAutorización(autorizaciónClave).* Habiendo el terminal T1 recibido el testigo de autorización, el acceso por el terminal T1 a los datos del usuario U2 es, desde ese momento, posible (recuadro E36) con la condición de la presentación por el terminal T1 del testigo de autorización al servidor AUT, el usuario U1 podrá consultar, entonces, los datos personales del usuario U2.

REIVINDICACIONES

1. Procedimiento de acceso por un primer terminal de telecomunicación (T1) a una base de datos (SVR) alojada por una plataforma de servicios (PTF) accesible mediante una red de telecomunicaciones (RED), que comprende:

(A) - la transmisión (E10, E12) de una información representativa de una petición de acceso del primer terminal a la base de datos, con destino a un segundo terminal (T2) asociado a un identificador de abonado a una segunda red de telecomunicaciones, correspondiendo dicho identificador de abonado al segundo terminal;
(B) - en el segundo terminal (T2), el envío (E14) de una respuesta a dicha petición de acceso con destino a un servidor de autenticación (AUT) de dicha plataforma, comprendiendo dicha respuesta un identificador del primer terminal (T1) y el identificador de abonado del segundo terminal (T2);
(C) - en el servidor de autenticación (AUT), cuando se recibe una respuesta a la petición de acceso, la verificación (E16) del identificador del abonado a dicha segunda red y la validación (E16) o no del acceso a la base de datos por el primer terminal en función del resultado de dicha verificación.

2. Procedimiento según la reivindicación 1, en el que la etapa (A) comprende:

(a1) - en el primer terminal (T1) de telecomunicación, generación (E10) de una petición de acceso a la base de datos, constando dicha petición de una información de identificación de dicho abonado a la segunda red de telecomunicaciones y envío de la petición de acceso al servidor de autenticación de la plataforma;
(a2) - en el servidor de autenticación (AUT), determinación (E12) del segundo terminal de telecomunicación a partir de dicha información de identificación de abonado extraída de la petición de acceso recibida, luego, transmisión (E12) al segundo terminal (T2) de una solicitud de autorización de acceso del primer terminal a la base de datos.

3. Procedimiento según la reivindicación 2, en el que la etapa (B) comprende:

(b1) - notificación de la solicitud de autorización de acceso en el segundo terminal; y
(b2) - como continuación a una acción de un usuario del segundo terminal efectuada por medio de una interfaz hombre-máquina del segundo terminal, envío de una respuesta a la solicitud de autorización de acceso con destino al servidor de autenticación.

4. Procedimiento según la reivindicación 2 o 3, en el que la red de telecomunicaciones es una red de tipo Internet y en el que la etapa (A) consta de una operación previa de carga y de visualización en el primer terminal de una página web de acceso al servidor de autenticación de dicha plataforma, siguiendo la petición de acceso al servidor de autenticación a un comando del usuario del primer terminal transmitido mediante dicha página web.

5. Procedimiento según una cualquiera de las reivindicaciones 2 a 4, que comprende la visualización en el segundo terminal de una interfaz gráfica que visualiza unas informaciones relativas a las solicitudes de acceso y al estado de conexión con la plataforma de servicios para un conjunto de terminales de telecomunicaciones predeterminado.

6. Procedimiento según la reivindicación 2, en el que, para una lista predeterminada de primeros terminales identificados en una lista almacenada en el segundo terminal, el segundo terminal envía automáticamente una respuesta a la petición de acceso recibida con destino al servidor de autenticación.

7. Procedimiento según la reivindicación 2, en el que, para una lista predeterminada de primeros terminales identificados en una lista almacenada en el servidor de autenticación, la etapa (a2) de transmisión al segundo terminal de una solicitud de autorización de acceso del primer terminal a la base de datos no se implementa cuando dicho primer terminal se identifica como que es un terminal de dicha lista, siendo el acceso del primer terminal a la base de datos validado automáticamente.

8. Procedimiento según la reivindicación 1, que comprende una operación previa de carga y de visualización en el primer terminal de una página web de acceso al servidor de autenticación de dicha plataforma y en el que:

- dicha página web de acceso al servidor de autenticación de la plataforma de servicios, visualizada en una pantalla del primer terminal, representa un código de dos dimensiones generado automáticamente por el servidor de autenticación durante la descarga de dicha página web;
- la etapa (A) de transmisión de una información representativa de una petición de acceso a dicha base de datos del primer terminal al segundo terminal, consiste en transmitir dicho código de dos dimensiones a una aplicación de software instalada en el segundo terminal.

9. Procedimiento según la reivindicación 8, en el que, en la etapa (B), la respuesta a la petición de acceso enviada del segundo terminal con destino al servidor de autenticación consta de dicho código de dos dimensiones, comparando el servidor de autenticación, a continuación, el código recibido con el código generado inicialmente.

10. Terminal de telecomunicaciones (T2) que comprende;

- unos medios (E/S) de recepción de una información representativa de una petición de acceso de un primer terminal de telecomunicación (T1) a una base de datos alojada por una plataforma de servicios (PTF) en una red de telecomunicaciones (RED);
- unos medios (APLI2) de generación y de envío de una respuesta a dicha petición de acceso con destino a un servidor de autenticación de dicha plataforma, con el fin de verificar un identificador de abonado a una segunda red de telecomunicaciones, correspondiendo dicho identificador de abonado al segundo terminal, al que está conectado dicho terminal de telecomunicación, comprendiendo dicha respuesta un identificador del primer terminal (T1) y el identificador de abonado del segundo terminal (T2) y de validar el acceso a la base de datos por el primer terminal en función del resultado de dicha verificación.

11. Terminal según la reivindicación 10, que incluye, además, unos medios de interfaz hombre-máquina adaptados para notificar a un usuario del terminal dicha información representativa de la petición de acceso y para enviar una respuesta a la petición de acceso con destino a un servidor de autenticación, como continuación a una acción de dicho usuario efectuada mediante la interfaz hombre-máquina.

12. Terminal según una de las reivindicaciones 10 u 11, que incluye unos medios de interfaz gráfica adaptados para visualizar unas informaciones relativas a las peticiones de acceso y al estado de conexión con la plataforma de servicios para un conjunto de terminales de telecomunicaciones predeterminado.

13. Servidor de autenticación (AUT) para la implementación de un procedimiento de acceso a una base de datos, de acuerdo con una cualquiera de las reivindicaciones 1 a 9, comprendiendo dicho servidor:

- unos medios (E/S-A) de recepción de una respuesta a una petición de acceso de un primer terminal de telecomunicación (T1) a dicha base de datos, que proviene de un segundo terminal de telecomunicación (T2), comprendiendo dicha respuesta un identificador del primer terminal (T1) y un identificador de abonado del segundo terminal (T2); y
- unos medios (APLI-A) de verificación del identificador de abonado a una segunda red de telecomunicaciones que corresponde al segundo terminal como continuación a la recepción de dicha respuesta a una petición de acceso y de validación del acceso a la base de datos por el primer terminal en función del resultado de dicha verificación.

14. Servidor según reivindicación 13, que incluye, además:

- unos medios de recepción de una petición de acceso a la base de datos que proviene del primer terminal, constando dicha petición de una información de identificación de un abonado a una segunda red de telecomunicaciones;
- unos medios de determinación de un segundo terminal de telecomunicación a partir de dicha información de identificación de abonado extraída de la petición de acceso recibida; y,
- unos medios de transmisión al segundo terminal de una solicitud de autorización de acceso del primer terminal a la base de datos.

15. Módulo de software incorporado en un terminal de telecomunicación según una cualquiera de las reivindicaciones 10 a 12 o en un servidor de autenticación según la reivindicación 13 o 14, incluyendo dicho módulo de software unas instrucciones de programa cuya ejecución por un procesador informático permite implementar un procedimiento de acceso a una base de datos, según una cualquiera de las reivindicaciones 1 a 9.

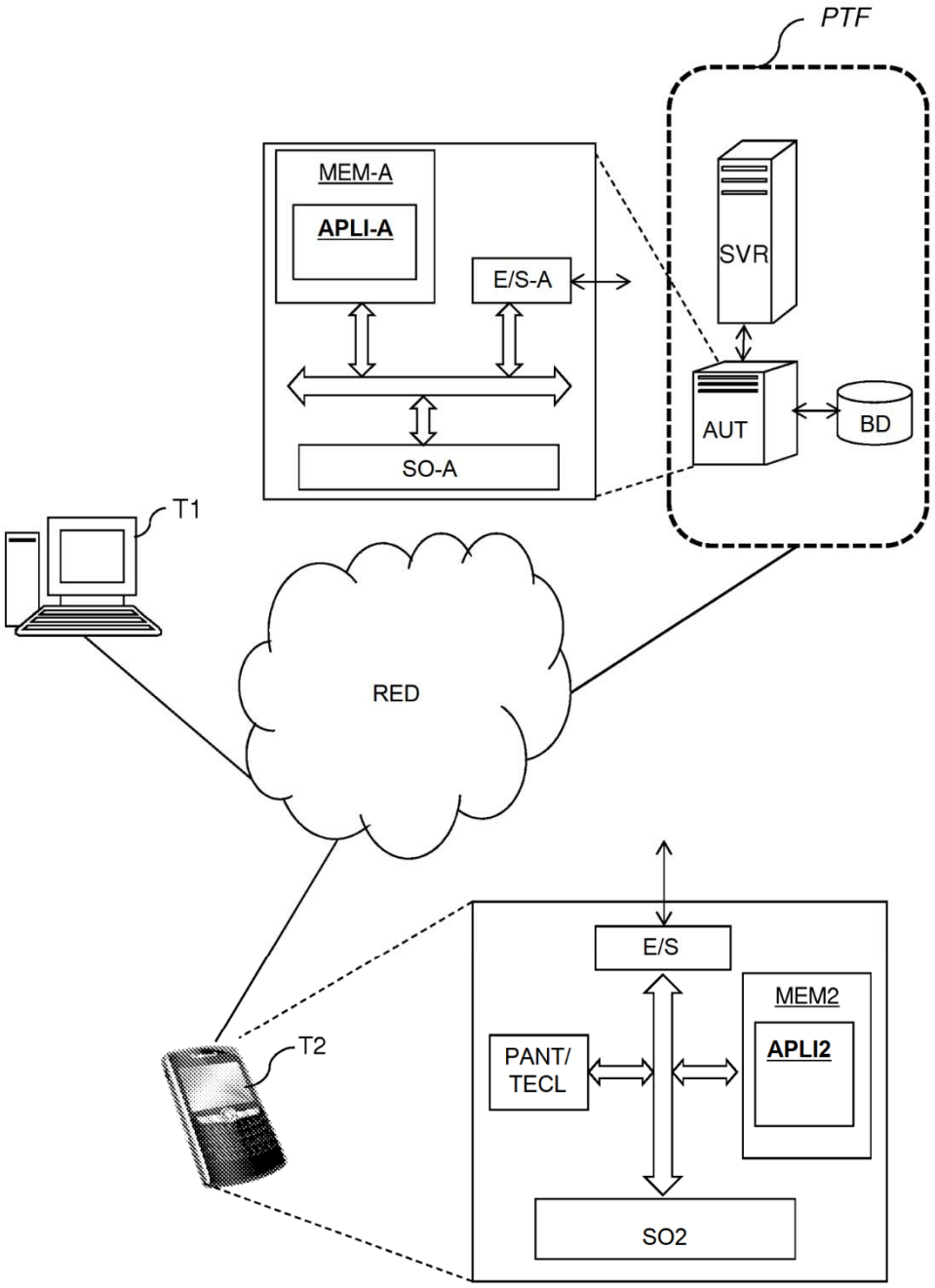
PTF
MEM-A
APLI-A
E/S-A
SO-A
SVR
AUT
BD
T1
RED
T2
E/S
MEM2
APLI2
PANT/
TECL
SO2

FIG. 1

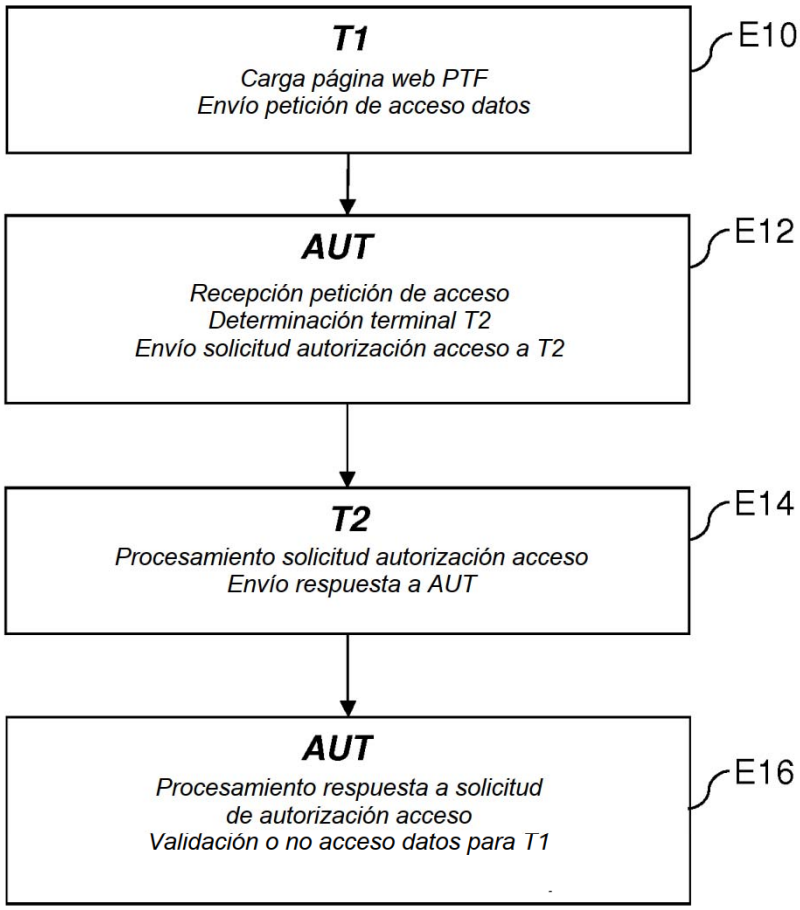
T1
Carga página web PTF
Envío petición de acceso datos
E10
AUT
Recepción petición de acceso
Determinación terminal T2
Envío solicitud autorización acceso a T2
E12
T2
Procesamiento solicitud autorización acceso
Envío respuesta a AUT
E14
AUT
Procesamiento respuesta a solicitud
de autorización acceso
Validación o no acceso datos para T1
E16

FIG. 2

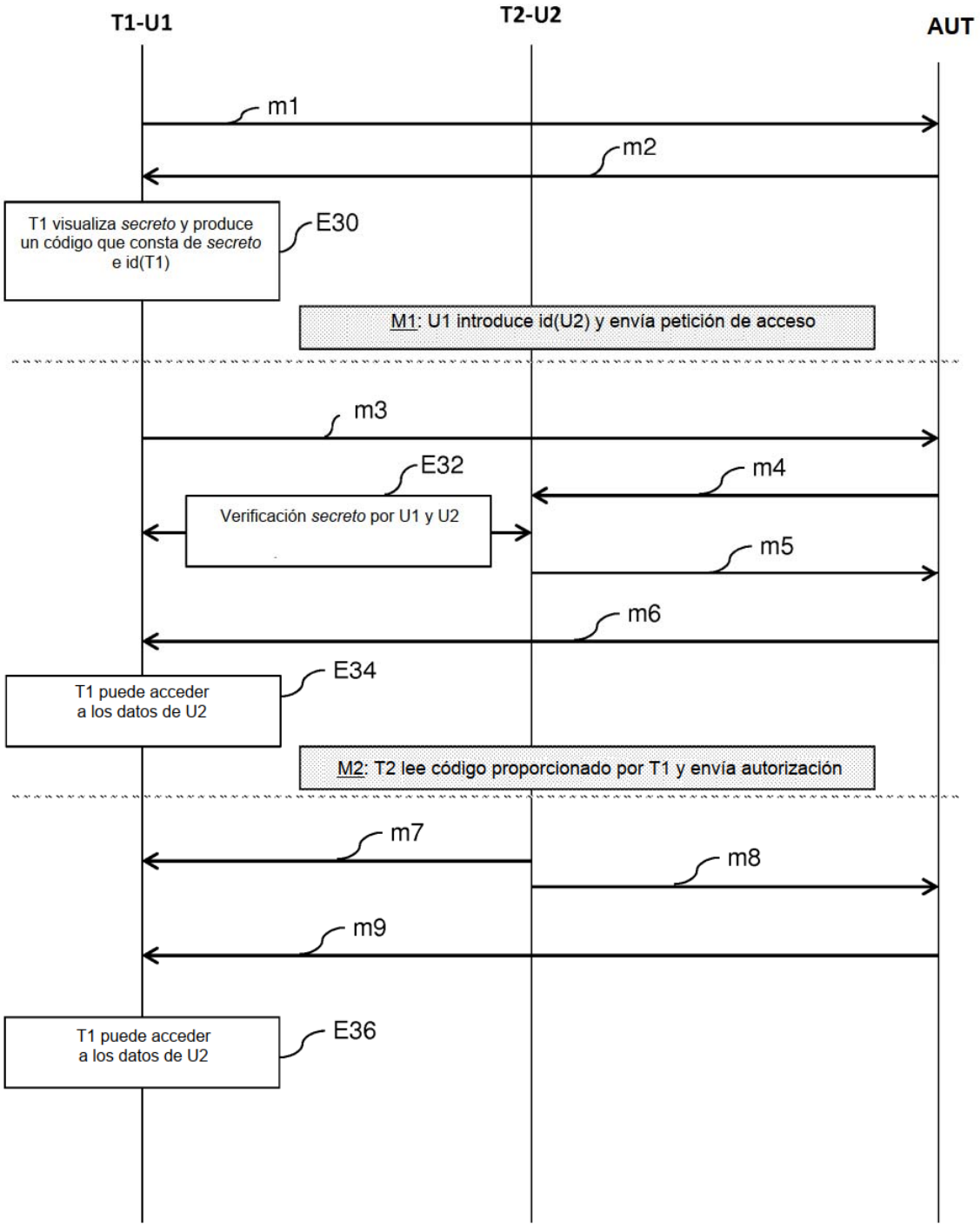
T1-U1
T2-U2
AUT
m1
m2
T1 visualiza *secreto* y produce un código que consta de *secreto* e id(T1)
E30
M1: U1 introduce id(U2) y envía petición de acceso
m3
E32
m4
Verificación *secreto* por U1 y U2
m5
m6
T1 puede acceder a los datos de U2
E34
M2: T2 lee código proporcionado por T1 y envía autorización
m7
m8
m9
T1 puede acceder a los datos de U2
E36

FIG. 3