(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 606 726**

(51) Int. CI.:

G06F 21/62 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.02.2014 E 14156392 (4)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2911083**

(54) Título: **Método de acceso a los datos de al menos una persona física o moral o de un objeto**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.03.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

BOCCHETTI, SALVATORE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de acceso a los datos de al menos una persona física o moral o de un objeto

Introducción

[0001] La presente solicitud se refiere al dominio de la protección de los datos privados, en particular los datos almacenados en bases de datos utilizadas con fines de autentificación.

[0002] Puede ser interesante que unos datos sean accesibles con el fin de permitir a terceras personas autorizadas obtener informaciones fiables con el fin de acceder a los servicios.
Este puede ser el caso para la adquisición de un crédito, procedimiento durante el cual las capacidades financieras del solicitante deben ser verificadas.
Otras aplicaciones pueden concernir la edad de la persona, sus competencias.
Puede también tratarse de las características de un objeto como rendimiento, tamaño, capacidad.

[0003] El problema que mantienen tales verificaciones es que el acceso a estos datos es abierto a la entidad solicitante en el momento del procedimiento de verificación.

[0004] Es desde entonces deseable que estos datos básicos, propios de una persona o un objeto, sean utilizados sin ser divulgados, por ejemplo, para asegurar la conformidad de la persona o del objeto a las condiciones definidas por una entidad solicitante.

[0005] Además, la conformidad a una solicitud o a las condiciones requeridas por la entidad solicitante debe poder ser validada por una autoridad de manera que la respuesta entregada por la entidad respondedora pueda ser fiable sin tener que divulgar los datos brutos.

Estado de la técnica

[0006] El documento WO2008/122627 describe una solución de verificación centrada en un usuario.
La tarjeta SIM almacena las informaciones personales y un tercero tal como un distribuidor de cigarrillos puede interrogar la tarjeta SIM a través del teléfono móvil de un usuario.
La máquina automática puede formar una solicitud, certificarla y transmitirla al teléfono móvil.
Este último, a través de la tarjeta protegida SIM puede ejecutar la solicitud (verificar si la edad del abonado es adecuada) y reenviar una respuesta.

Breve descripción de la invención

[0007] La presente invención se refiere a proponer un método y un sistema que permita proporcionar informaciones fiables, certificadas, sin que la fuente de las informaciones sea transmitida al solicitante.

[0008] La presente invención propone un método de acceso a los datos de al menos una persona física o moral o de un objeto, almacenados en una base de datos protegida en un soporte extraíble, estos datos comprendiendo datos cuantitativos o cualitativos, cada dato comprendiendo al menos un descriptor y un valor, este método comprendiendo las etapas de inicialización y de explotación, la inicialización comprendiendo las etapas siguientes:
* conectar el soporte extraíble a un dispositivo de recogida de informaciones,
* autenticarse ante la base de datos demostrando el derecho a al menos una introducción,
* introducir en la base de datos protegida, para una persona moral o física o un objeto, un valor corriente correspondiente al descriptor de dicho dato;
la explotación comprendiendo las etapas siguientes:
* conectar el soporte extraíble en un dispositivo de comunicación,
* recibir una solicitud de una entidad participante, esta solicitud comprendiendo al menos un descriptor meta y un operador,
* ejecutar, por la entidad respondedora, la solicitud aplicando el operador sobre el valor corriente correspondiente al descriptor meta y producir una respuesta,
* reenviar la respuesta a la entidad participante, caracterizada por el hecho de que la base de datos comprende de más a menos un contador de solicitudes asociado a uno o varios datos, y comprendiendo las etapas de:
* comparar el valor del contador con un valor máximo, la ejecución de la solicitud y el reenvío de la respuesta siendo ejecutados solo si el valor es inferior al valor máximo.

[0009] Así la presente invención se basa en un soporte extraíble tal como una tarjeta inteligente, un teléfono móvil o cualquier elemento electrónico que disponga de capacidad de memoria, almacenando los datos de una persona física o moral o de un objeto.
Por persona física se entiende un individuo o un grupo de individuos tales como una familia.
Una persona moral puede ser una empresa, una asociación, una organización.
Un objeto dispone también de características que se pueden utilizar para autentificación.

[0010] La presente invención propone un método de acceso limitado a los datos de una pluralidad de personas físicas o morales o de objetos, almacenados en una base de datos protegida de una entidad respondedora, estos datos comprendiendo los datos cuantitativos o cualitativos, cada dato comprendiendo al menos un descriptor y un valor, este método comprendiendo las etapas de inicialización y de explotación, la inicialización comprendiendo las etapas siguientes:
- autenticarse ante la base de datos demostrando el derecho con al menos una introducción,
- identificar al menos una persona o un objeto,
- introducir en la base de datos protegida, para dicha persona u objeto, un valor corriente correspondiente al descriptor de dicho dato,
la explotación comprendiendo las etapas siguientes:
- recibir una solicitud de una entidad participante, esta solicitud comprendiendo un identificador de persona o de objeto, un descriptor meta, un operador,
- ejecutar, por la entidad respondedora, la solicitud aplicando el operador sobre el valor corriente correspondiente al descriptor meta y producir una respuesta,
- reenviar la respuesta a la entidad participante, caracterizada por el hecho de que la base de datos comprende de más a menos un contador de solicitudes asociado a uno o varios datos, y comprendiendo las etapas de:
    - comparar el valor del contador con un valor máximo, la ejecución de la solicitud y el reenvío de la respuesta se ejecutan solo si el valor es inferior al valor máximo.

[0011] Así este método comprende una primera etapa de inicialización, comprendiendo la introducción de los datos, y una segunda etapa de explotación, comprendiendo la recepción, el tratamiento y la respuesta a las solicitudes.

[0012] La invención propone igualmente un soporte extraíble como se describe en las reivindicaciones.

Breve descripción de las figuras

[0013] La presente solicitud se comprenderá mejor sobre la base de las figuras anexas en las cuales:
- la figura 1 ilustra los diferentes elementos componentes de la invención.

Descripción detallada

[0014] El método se articula alrededor de una entidad respondedora ENP que dispone de una base de datos DB pudiendo almacenar datos privados de persona física o moral o de un objeto.
Los datos son habitualmente organizados en forma de registro, sea un conjunto de datos conectado por una definición común.

[0015] Cada registro incluye al menos un descriptor (por ejemplo, salario, profesión, edad, dirección, etc) y un valor correspondiente a dicho descriptor.
Opcionalmente, un certificado se asocia a uno o varios registros.

[0016] Un ejemplo de certificado es conocido bajo la denominación X.509.
En el sistema X.509, una autoridad de certificación atribuye un certificado que asocia una clave pública a un nombre distintivo (Distinguished Name), a una dirección electrónica o un registro DNS.

[0017] Este certificado coloca la firma de una autoridad de certificación en el último campo.
Concretamente esta firma es realizada por: Un condensado de todos los campos precedentes del certificado, y un cifrado de este condensado por la clave privada de la autoridad de certificación.
Quienquiera que posea la clave pública de esta autoridad de certificación puede descifrar el condensado y compararlo con el cálculo de su propio condensado del certificado.
Si los dos condensados son idénticos esto garantiza que el certificado es íntegro, no ha sido modificado.
El certificado de la autoridad de certificación que contiene su clave pública puede a su vez ser firmado por otro certificado de más alto nivel, formando así una cadena.
Arriba del todo de la cadena se encuentran los certificados más importantes: los certificados raíces.
Los certificados raíces son las claves públicas no firmadas, o autofirmadas, en las cuales se basa la confianza.
Los software, como los navegadores Web o los clientes de mensajería guardan los certificados raíces de numerosas autoridades de certificación comerciales o gubernamentales.
Cuando un navegador abre una conexión protegida (TLS/SSL) hacia un sito que posee un certificado emitido por una autoridad conocida, considera el sito como seguro en la medida en que la ruta de certificación es validada.
El paso en modo protegido es entonces transparente.

[0018] En el momento de una etapa de inicialización, una persona moral (una sociedad, una organización) o una persona física puede almacenar los datos privados en la base de datos de la entidad respondedora.
En el caso de datos relativos a un objeto, los datos se pueden almacenar de manera automática (por ejemplo, valores capturados por una sonda).

El almacenamiento puede también ser tipo temporal, por ejemplo, en el caso en el que los datos se capturan por una sonda conectada a una memoria que actúa de “base de datos”.
La entidad respondedora puede ser un soporte extraíble comprendiendo una memoria y medios de tratamiento de las solicitudes.
Este puede ser un teléfono móvil por ejemplo, conectado temporalmente a una entidad solicitante por enlace Bluetooth o NFC.

[0019] La base de datos puede comprender dos tipos de descriptor, sea aquellos predefinidos y aquellos definidos por la persona.

[0020] En la primera categoría, se encuentran todos los registros predefinidos para los cuales bastará rellenar el valor meta.
Se trata de datos corrientes como la fecha de nacimiento, la dirección, la situación familiar o la renta.

[0021] El descriptor del registro es por lo tanto un sencillo valor que hace referencia a una lista de definición (por ejemplo, el valor 27 del descriptor significa que el valor meta es el año de nacimiento).

[0022] El descriptor puede ser un campo editable libre.
Así la persona puede definir los tipos de datos no previstos por la entidad respondedora ENR y asociarle el valor de su elección.

[0023] La base de datos de la entidad respondedora es protegida es decir que la introducción de los datos no puede hacerse sin autorización.
La base de datos es protegida por una autentificación fuerte como el uso de una contraseña de uso único, el uso de un certificado electrónico, o el uso de datos biométricos.

[0024] Según un procedimiento de certificación, los datos son a continuación certificados por una autoridad AUT que se ilustra como una entidad diferenciada en la figura 1.
Esta autoridad se puede integrar en la entidad respondedora o ser una entidad separada.

[0025] El procedimiento de certificación consiste en hacer intervenir un tercero que podrá confirmar la información.
Esta autoridad AUT puede obtener a través de otras fuentes informaciones para corroborar el valor inscrito en la base de datos.
En efecto, las sociedades especializadas disponen de informaciones fiables sobre las personas o las sociedades y pueden certificar uno o varios valores.
Por ejemplo, sobre la solicitud de la persona, la entidad respondedora ENR puede acceder a esta autoridad AUT que está en forma de un servicio especializado (por ejemplo, un banco para verificar el límite de crédito).
Previamente, la entidad respondedora puede pedir a la persona informaciones complementarias como contraseña o información de verificación.
Estas informaciones complementarias serán agregadas a la solicitud transmitida a la autoridad con el fin de permitir a esta autoridad de verificar la legitimidad de la solicitud.
Esta autoridad dispone de un certificado para firmar el valor transmitido en la solicitud.
En la medida en que la base de datos se realiza con un elemento protegido, que no permite la extracción de información más allá de la que se considera que forma parte de comunicación hacia el exterior (ej. tarjeta inteligente,...), la autoridad AUT comunicará su certificado al elemento protegido para que este último pueda utilizarlo para firmar la respuesta proporcionada.
En otra realización, el elemento protegido utilizará para la firma otro certificado que ha sido a su vez verificado y firmado por una autoridad AUT-

[0026] Así la base de datos de la entidad respondedora incluirá los registros organizados con un descriptor de datos y uno o varios valores así como uno o varios certificados asociados a las autoridades.

[0027] En un segundo tiempo, una entidad solicitante ENP1, ENP2 puede formar una solicitud para obtener una verificación de una información.
Esta solicitud comprenderá un identificador de entidad solicitante, el descriptor de datos (por ejemplo, la renta), un operador (por ejemplo < o >) y de forma accesoria un valor meta.
El valor meta puede ser opcional, por ejemplo en el momento de la verificación del acceso a un bar, basta que el descriptor sea "la edad" y el operador sea "¿mayor de edad ?".
Una solicitud puede comprender varios descriptores (por ejemplo, la ciudad de residencia y la calle) y/o varios valores meta (por ejemplo, una lista de supuestos empleadores).
Esta solicitud puede ser igualmente firmada por la entidad solicitante para autenticar la solicitud.

[0028] A la recepción de esta solicitud, la entidad respondedora va a poder determinar la persona a quien se dirige esta solicitud gracias al identificador, y recuperará el dato en cuestión a través del descriptor y recuperará el valor correspondiente a este dato.

[0029] La entidad respondedora a continuación aplicará el operador sobre el valor y obtendrá una respuesta.
Esta respuesta será principalmente binaria sea positivo o negativo o un rechazo de respuesta.
La respuesta puede ser igualmente contener una firma agregada a esta respuesta.
Esta respuesta se envía a la entidad solicitante.
La respuesta puede comprender una copia de la pregunta a saber el valor meta, el operador, el identificador de la persona.

[0030] Según una variante de la invención, cuando una solicitud es recibida por la entidad respondedora, esta entidad transmite la solicitud o una parte a la persona correspondiente al identificador de persona.
Esta solicitud se presenta a un dispositivo de visualización de la persona.
De esta manera se presenta un identificador de la entidad solicitante, y los detalles de la solicitud.
La persona puede aceptar o rechazar que una respuesta sea enviada a la entidad solicitante, pero no puede modificar la respuesta si el envío ha sido autorizado por la persona

[0031] Según una variante de la invención, el tratamiento de la solicitud difiere en función de la entidad solicitante.
La entidad respondedora va a determinar la categoría a la cual pertenece esta entidad solicitante, y según esta categoría algunos de los datos serán accesibles o no.
La base de datos DB comprende una lista de las entidades solicitantes posibles y su categoría.
Una institución estatal será por ejemplo de categoría 4 (de alto valor de confianza) mientras que una simple tienda será categoría 1 (nivel de confianza bajo).
De la misma manera, los datos de la persona física o moral se pueden clasificar según las categorías, permitiendo de este modo, en el momento de una solicitud, verificar si la categoría a la cual pertenece la entidad solicitante autoriza el acceso a este dato.
Si el nivel unido a los datos es igual o inferior al nivel de la entidad solicitante, la solicitud es tratada y la respuesta es enviada.
En caso contrario, una respuesta de denegación de la solicitud es enviada a la entidad solicitante por la entidad respondedora.

[0032] Un método conocido para extraer los datos brutos de una tal base de datos es enviar una multitud de solicitudes haciendo variar el valor meta.
Así por ejemplo si la renta es el objetivo, una solicitud que pregunta si la renta es inferior a un primer valor meta se envía y cuando la respuesta es positiva, el valor meta es incrementado.
Así el valor de la renta corresponde al momento en el que la respuesta cambia.
Gracias a este método recurrente, es posible conocer todos los valores de la base de datos.

[0033] Así según la invención, un contador de solicitudes se añade a la entidad respondedora y permite limitar el número de solicitudes.
El contador se puede asociar al conjunto de los datos de una persona, a un dato de una persona, o a una entidad solicitante, o a un conjunto de los parámetros citados.
Para tomar el tercer ejemplo, en cada solicitud de una entidad solicitante particular, el contador es incrementado.
Un máximo se define para el contador y cuando este máximo se alcanza, la entidad respondedora rechaza las solicitudes siguientes.
El contador podrá ser vuelto a poner a cero por un operador de la entidad respondedora o por la persona.

[0034] El control por el contador se puede asociar a un máximo por unidad de tiempo, por ejemplo 3 solicitudes cada 24 horas.
Una vez este número es alcanzado durante el tiempo predefinido, las solicitudes siguientes son rechazadas.
Una vez el período ha expirado, el contador se vuelve a poner a cero.

REIVINDICACIONES

1. Método de acceso a los datos personales de por lo menos una persona física o moral o de un objeto, almacenados en una base de datos protegida en un soporte extraíble, estos datos comprendiendo los datos cuantitativos o cualitativos, cada dato comprendiendo al menos un descriptor y un valor, este método comprendiendo las etapas de inicialización y de explotación, la inicialización comprendiendo las etapas siguientes:
- conectar el soporte extraíble a un dispositivo de recogida de informaciones,
- autenticarse ante la base de datos demostrando el derecho con al menos una introducción,
- introducir en la base de datos protegida, para una persona moral o física o un objeto, un valor corriente correspondiente al descriptor de dicho dato;
la explotación comprendiendo las etapas siguientes:
- conectar el soporte extraíble a un dispositivo de comunicación,
- recibir una solicitud de una entidad solicitante, esta solicitud comprendiendo al menos un descriptor meta y un operador,
- ejecutar, por la entidad respondedora, la solicitud aplicando el operador sobre el valor corriente correspondiente al descriptor meta y producir una respuesta,
- reenviar la respuesta a la entidad solicitante, la base de datos comprendiendo de más a menos un contador de solicitudes asociado a uno o varios datos, y el método comprendiendo las etapas de:
- comparar el valor del contador con un valor máximo, la ejecución de la solicitud y el reenvío de la respuesta solo se ejecutan si el valor es inferior al valor máximo.

2. Método de acceso limitado a los datos de una pluralidad de personas físicas o morales o de objetos, almacenados en una base de datos protegida de una entidad respondedora, estos datos comprendiendo los datos cuantitativos o cualitativos, cada dato comprendiendo al menos un descriptor y un valor, este método comprendiendo las etapas de inicialización y de explotación, la inicialización comprendiendo las etapas siguientes:
- autenticarse en la base de datos demostrando el derecho con al menos una introducción,
- identificar al menos una persona o un objeto,
- introducir en la base de datos protegida, para dicha persona u objeto, un valor corriente correspondiente al descriptor de dicho dato,
la explotación comprendiendo las etapas siguientes:
- recibir una solicitud de una entidad solicitante, esta solicitud comprendiendo un identificador de persona o de objeto, un descriptor meta, un operador,
- ejecutar, por la entidad respondedora, la solicitud aplicando el operador sobre el valor corriente correspondiente al descriptor meta y producir una respuesta,
- reenviar la respuesta a la entidad solicitante, la base de datos comprendiendo de más a menos un contador de solicitudes asociado a uno o varios datos, y el método comprendiendo las etapas de:
- comparar el valor del contador con un valor máximo, el cumplimiento de la solicitud y el reenvío de la respuesta solo se ejecutan si el valor es inferior al valor máximo.

3. Método según la reivindicación 1 o 2, caracterizado por el hecho que comprende una etapa de certificación, comprendiendo la conexión de un certificado emitido por una autoridad a un dato de la base de datos, y por el hecho de que dicho certificado se utiliza en la preparación de la respuesta enviada a la entidad solicitante.

4. Método según la reivindicación 1 o 2, caracterizado por el hecho de que la entidad solicitante dispone de un certificado, dicho certificado siendo utilizado para firmar la solicitud enviada a la entidad respondedora, dicho certificado siendo verificado antes de poder ejecutar la solicitud.

5. Método según la reivindicación 1 o 2, caracterizado por el hecho de que el descriptor es tipo índice, un valor de índice correspondiendo a un tipo de descriptor.

6. Método según la reivindicación 1 o 2, caracterizado por el hecho de que el descriptor es tipo campo libre, el contenido del campo libre siendo inicializado en el momento de la introducción del valor corriente en la base de datos, la entidad respondedora, en el momento de la recepción del descriptor meta de la solicitud efectúa una búsqueda por comparación entre el descriptor meta y el o los contenidos del o de los descriptores de dicha base de datos.

7. Método según la reivindicación 1 o 2, caracterizado por el hecho de que comprende las etapas siguientes:
- una vez la solicitud es recibida por la entidad respondedora, transmitir un mensaje a la persona identificada por el identificador de persona, este mensaje conteniendo al menos el descriptor meta,
- visualizar sobre un dispositivo de la persona el descriptor meta,
- recepción de un control por parte de la persona, este control autoriza o prohíbe la solicitud,
- transmisión del control a la entidad respondedora,
- autorización o prohibición del tratamiento de la solicitud según el valor del control.

8. Método según la reivindicación 7, caracterizado por el hecho de que la solicitud comprende un identificador de la entidad solicitante, y por el hecho de que este identificador se visualiza sobre el dispositivo de la persona con el descriptor meta.

9. Método según la reivindicación 1 o 2, caracterizado por el hecho de que la solicitud comprende un identificador de entidad solicitante, y por el hecho de que comprende las etapas siguientes:
- organizar los datos de una persona según al menos dos categorías,
- determinar a qué categoría pertenece la entidad solicitante,
- aceptar una solicitud siempre y cuando la categoría de la entidad solicitante sea compatible con la categoría de los datos del descriptor meta.

10. Soporte extraíble asociado con al menos una persona física o moral o de un objeto y comprendiendo una base de datos protegida, comprendiendo los datos cuantitativos o cualitativos, cada dato comprendiendo al menos un descriptor y un valor y al menos un contador de solicitudes asociado a uno o varios datos, dicho soporte extraíble pudiendo estar en un estado de inicialización o de explotación, dicho soporte extraíble estando configurado para, en el estado de inicialización, ser conectado a un dispositivo de recogida de informaciones, recibir los datos de autentificación demostrando el derecho con al menos una introducción en dicha base de datos, e introducir en la base de datos protegida, para una persona moral o física o un objeto, un valor corriente correspondiente al descriptor de dicho dato; dicho soporte extraíble estando configurado para, en el estado de explotación, ser conectado a un dispositivo de comunicación, recibir una solicitud de una entidad participante, esta solicitud comprendiendo al menos un descriptor meta y un operador, comparar el valor del contador con un valor máximo, si el valor es inferior, incrementar el contador en cada solicitud ejecutada por la entidad respondedora, y ejecutar, por la entidad respondedora, la solicitud aplicando el operador sobre el valor corriente correspondiente al descriptor meta y producir una respuesta, y reenviar la respuesta a la entidad solicitante.

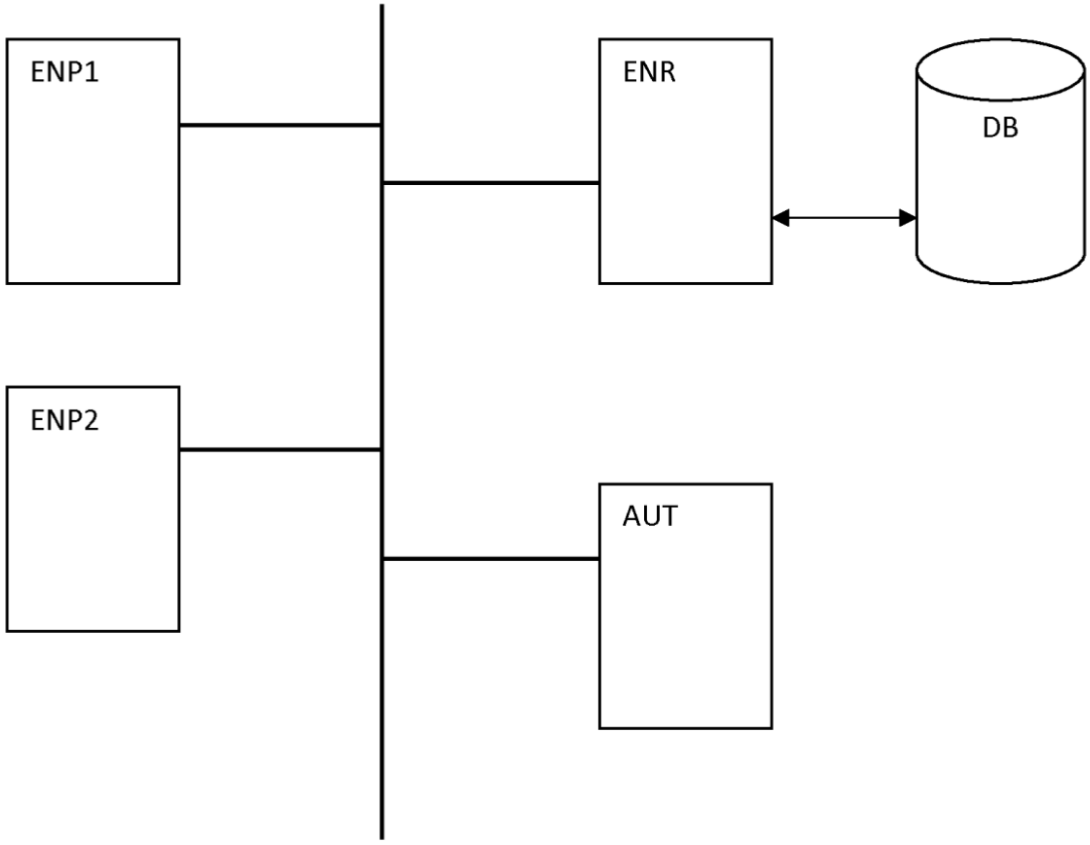

Fig. 1