(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 368 148**

(51) Int. CI.:
G06F 17/30 (2006.01)
H04M 3/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04809220 .9**
(96) Fecha de presentación: **29.12.2004**
(97) Número de publicación de la solicitud: **1839194**
(97) Fecha de publicación de la solicitud: **03.10.2007**

(54) Título: **INTERCEPTACIÓN DE BASES DE DATOS.**

(45) Fecha de publicación de la mención BOPI:
14.11.2011

(45) Fecha de la publicación del folleto de la patente:
14.11.2011

(73) Titular/es:
Telefonaktiebolaget L- M Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
IMBIMBO, Amedeo

(74) Agente: **de Elzaburu Márquez, Alberto**

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

Interceptación de bases de datos

Campo técnico de la invención

La presente invención se refiere a los métodos y las adaptaciones en un sistema de comunicación para proporcionar información relacionada con el uso de un objeto de directorio en una base de datos.

Descripción de la técnica relacionada

En las redes de comunicación modernas las distintas bases de datos son elementos importantes. Proporcionan soporte para todo tipo de aplicaciones que se podrían distribuir en distintos Servidores de Aplicaciones. Un ejemplo de datos son los datos de usuario para un abonado, por ejemplo si el usuario tiene activado un servicio de desvío de llamadas.

Un ejemplo de una base de datos en una red de comunicación es el Servidor Local de Abonado. Es, como se define en la R6 del 3GPP, la base de datos maestra para los usuarios de GSM y WCDMA. Proporciona soporte para la seguridad, autorización, gestión de la movilidad, itinerancia, identificación y aprovisionamiento de servicios del usuario para el dominio de Circuitos Conmutados (CS), para el dominio de Paquetes Conmutados (PS), para acceso WLAN a WCDMA (como se define en la R6 del 3GPP) y para el subsistema Multimedia IP. El Servidor Local de Abonado se podría usar para cualquier aplicación desarrollada en la Capa de Servicios. Un Servidor de Aplicaciones en la Capa de Servicios podría pedir y recibir datos, para la ejecución de un cierto servicio, desde el Servidor Local de Abonado, por ejemplo qué tipo de servicio está activado en la suscripción de usuarios.

Un abonado puede tener la posibilidad de modificar sus datos de usuario (por ejemplo la activación del servicio de desvío de llamadas) marcando un código o número específico. La señalización desde el equipo de usuario a la base de datos va a través del intercambio local en caso de una línea fija o del nodo MSC en el caso de un usuario móvil.

También es posible permitir al usuario, el abonado, tener acceso a sus datos de usuario en un servidor de base de datos a través de un Servidor de Aplicaciones en la Capa de Servicio. El acceso al Servidor de Aplicaciones podría ser por ejemplo a través de Redes Internet. Los procedimientos entre el Servidor de Aplicaciones y el servidor de la base de datos se pueden ejecutar por medio de, por ejemplo, el protocolo LDAP o el interfaz Sh en base al Protocolo de Diámetro.

Hay una demanda para monitorizar el acceso y el uso de los servicios en una base de datos al mismo nivel de seguridad y confidencialidad que se conoce para los servicios de comunicación tradicional.

Una forma de monitorizar los Servicios de Comunicación es la Interceptación Legal, es decir el acto de interceptar una comunicación en favor de una Agencia Policial. La interceptación del Contenido de la Comunicación de las comunicaciones tradicionales es decir el habla y los datos es conocida. La interceptación de la Información Relacionada con la Interceptación también es conocida. La Información Relacionada con la Interceptación se define como la información de señalización relacionada con los abonados objetivo, por ejemplo el establecimiento de llamada. Como ejemplo, en el dominio de la Conmutación de Circuitos, el envío de la IRI a una función de monitorización se desencadena mediante los eventos relacionados con los siguientes eventos relacionados con llamadas y no relacionados con llamadas:

- Establecimiento de Llamada
- Respuesta
- Servicio Suplementario
- Traspaso
- Liberación
- Entrada Controlada del Abonado

Los eventos adecuados relacionados con la sesión y no relacionados con la sesión desencadenan el envío de la IRI a una función de monitorización en caso de comunicación de Conmutación de Paquetes.

Los procedimientos usados por el abonado para modificar sus datos de usuario en la base de datos (por ejemplo la activación del servicio de desvío de llamadas) son hoy en día interceptados en el intercambio local fijo para los abonados de línea fija o en el nodo MSC para los usuarios móviles.

De acuerdo con los estándares de Interceptación Legal actuales, no es posible informar, por medio de los eventos existentes de Información Relacionada con la Interceptación, el acceso y uso de servicios en una base de datos cuando se accede a la base de datos a través de un Servidor de Aplicaciones en la Capa de Servicio.

Resumen de la invención

La presente invención se refiere a los problemas de cómo generar información relacionada con el acceso y uso de un objeto de directorio en una base de datos.

Los problemas se resuelven mediante asociar un Punto de Acceso de Interceptación IAP al objeto de directorio en una base de datos y generar nueva información estructurada adecuadamente.

En más detalle los problemas se resuelven mediante un método de acuerdo con la reivindicación 1 y una adaptación de acuerdo con la reivindicación 9 en un sistema de comunicación para generar información relacionada con el uso del objeto de directorio monitorizado en una base de datos. El sistema proporciona la información a una Unidad de Configuración de Interceptación ICU. La información se recoge desde el IAP, el cual está asociado con el objeto de directorio monitorizado en el HSS. El método comprende los siguientes pasos:

- recibir en el Punto de Acceso de Interceptación IAP una petición para monitorizar el objeto de directorio en la base de datos,

- detección de uso del objeto de directorio monitorizado en el IAP,

- entregar la información relacionada con dicho uso, a partir del IAP a la Unidad de Configuración de Interceptación ICU.

Las ventajas de la invención son que se puede monitorizar el uso de un objeto de directorio en una base de datos.

La invención se describirá ahora más en detalle con la ayuda de las realizaciones preferentes en conexión con los dibujos adjuntos.

Breve descripción de los dibujos

La Figura 1 revela una ilustración esquemática de bloques de un sistema de comunicación que comprende un Servidor Local de Abonado HSS, un Servidor de Aplicaciones y una Unidad de Configuración de Interceptación ICU.

La Figura 2 revela una ilustración esquemática de bloques de una Unidad de Configuración de Interceptación ICU en el sistema de comunicación.

La Figura 3 revela un diagrama de flujo que ilustra algunos pasos esenciales del método de la invención.

Descripción detallada de las realizaciones

La Figura 1 revela un sistema de comunicación que comprende una Red de Servicio SN. La SN aloja un Servidor Local de Abonado HSS y un Servidor de Aplicaciones AS.

El Servidor de Aplicaciones AS podría alojar todo tipo de servicios y suscripción para un usuario. El Servidor Local de Abonado HSS es, como se define en la R6 del 3GPP, la base de datos maestra para los usuarios GSM y WCDMA. Proporciona soporte para la seguridad, la autorización, la gestión de movilidad, la itinerancia, la identificación y el aprovisionamiento de servicios del usuario para el dominio de Circuitos Conmutados (CS), para el dominio de Paquetes Conmutados (PS), para el acceso WLAN a WCDMA (como se define en la R6 del 3GPP) y para el subsistema Multimedia IP. El HSS se podría usar para cualquier aplicación desarrollada en la Capa de Servicio. Un Servidor de Aplicaciones en la Capa de Servicio podría pedir y recibir datos, para la ejecución de un cierto servicio, desde el HSS, por ejemplo qué tipo de servicio está activado en la suscripción de usuarios. Los datos para un usuario específico se almacenan bajo un objeto de directorio que tiene un nombre único, el nombre de directorio de HSS, es decir el nombre del perfil de abonado. Un objeto de directorio con el nombre de directorio de HSS HDN1 se almacena en el HSS. El HDN1 comprende al menos algunos datos de usuario para un abonado o usuario. El HSS se configura como un Punto de Acceso de Interceptación IAP.

El Servidor de Aplicaciones AS puede comunicar con el Servidor Local de Abonado HSS por medio del protocolo LDAP o Diámetro-Sh DSH. Otros protocolos también se podrían usar.

Una Unidad de Configuración de Interceptación ICU se conecta con el HSS/IAP. La ICU se conecta con el nodo a través de tres interfaces X1, X2 y X3. La ICU y los interfaces se explicarán más adelante en la figura 2.

La red de comunicación también comprende las Redes Internet IN. Un ordenador PC está conectado a las IN.

Un móvil WAP WM también está conectado a las Redes Internet IN a través de una estación base BS.

La Unidad de Configuración de Interceptación ICU se revela en la figura 2. La ICU comprende al menos una Agencia Policial LEA (tres bloques que representan distintas LEA se muestran en la figura 2). Cada LEA se conecta, a través de los interfaces H1-H3, a tres Funciones de Mediación respectivamente para ADMF, DF2 y DF3, es decir una Función de Administración ADMF y dos Funciones de Entrega, una denominada segunda Función de Entrega DF2 y la tercera Función de Entrega DF3. La LEA se conecta con la ADMF a través de un interfaz H1, a la DF2 a través del

interfaz H2 y a la DF3 a través del interfaz H3. La Función de Administración y las Funciones de Entrega se conectan cada una a la red de comunicación a través de los interfaces X1-X3. La ADMF está conectada a través del interfaz X1, la DF2 está conectada a través del X2 y la DF3 está conectada a través del X3. La Función de Administración ADMF se usa junto con las funciones de entrega para ocultarse de la red que pudiera tener múltiples activaciones por las diferentes Agencias Policiales. Los mensajes enviados desde la ADMF a la red a través del interfaz X1 comprenden las identidades del abonado/equipo que va a ser monitorizado, es decir las identidades objetivo. La segunda Función de Entrega DF2 recibe la Información Relacionada con la Interceptación IRI desde la red y la DF2 se usa para distribuir la IRI a las Agencias Policiales relevantes. La tercera Función de Entrega DF3 recibe el Contenido de la Comunicación CC, es decir el habla y los datos, y se usa para distribuir el CC a las LEA relevantes. La DF3 es responsable de la señalización de control de llamada y el trasporte portador para un producto interceptado.

La Información Relacionada con la Interceptación IRI, recibida por la DF2, se define como la información de la señalización relacionada con las suscripciones monitorizadas.

El envío de la Información Relacionada con la Interceptación IRI a una función de monitorización se desencadena mediante Eventos, éstos son o bien relacionados con la llamada o bien no relacionados con la llamada. El establecimiento de la llamada es un ejemplo de un Evento relacionado con la llamada y la actualización de la Ubicación es un ejemplo de un Evento no relacionado con la llamada. El acceso a un objeto de directorio, por ejemplo los datos de usuario de un abonado, en un HSS es un Evento que podría desencadenar el envío de la IRI a la ICU.

De acuerdo con una realización de la invención, se han mejorado los Eventos ya existentes para incluir también la monitorización de uso de un objeto de directorio en una base de datos, en este ejemplo un Servidor Local de Abonado HSS. Si un usuario accede a un objeto de directorio en el HSS, el Punto de Acceso de Interceptación IAP, es decir el HSS, envía los datos relevantes a la DF2. Esto se explicará más tarde en más detalle. Ejemplos de parámetros en el informe de la IRI cuando se accede a un objeto de directorio en el HSS son los siguientes:

- Protocolo de Acceso a HSS: El protocolo usado para acceder al objeto de directorio, por ejemplo LDAP o Diámetro SH

- Operación de HSS: Todas las operaciones del protocolo se transportarán en este parámetro, por ejemplo el Mensaje del LDAP en caso de LDAP o los Comandos en caso de Diámetro-Sh.

- Nombre de Directorio de HSS: El nombre del objeto de directorio al que se accede.

Se va a observar que esos parámetros anteriores son solamente ejemplos de posibles parámetros en el informe de la IRI relacionado con el acceso a un objeto de directorio en el HSS.

En esta realización de la invención el usuario tiene una suscripción de telefonía y al menos alguno de sus datos de usuario almacenados en el nombre de directorio de HSS HDN1. El usuario accede al HDN1 en el HSS a través de Redes Internet IN y un ordenador PC. Él activará el servicio de desvío de llamadas y envía sus llamadas de teléfono al número 12345. El objetivo de la interceptación será el nombre de directorio HDN1. El protocolo usado para acceder al HDN1 es LDAP en este ejemplo.

El HSS se configura como un IAP. El HDN1 se asocia al Punto de Acceso de Interceptación IAP, es decir el HSS.

Un método de acuerdo con esta realización de la invención se explicará ahora en más detalle. La explicación tiene que ser leída junto con la figura 1 y 2. El método comprende los siguientes pasos:

- La Agencia Policial LEA envía a través del interfaz H1 una petición a la Función de Administración ADMF para activar la interceptación de los datos de usuario almacenados en el Nombre de Directorio de HSS HDN1. Esto supone que el objeto de directorio HDN1 será monitorizado, será objetivo de la interceptación.

- La ADMF envía a través del interfaz X1 una identidad de objetivo del objeto de directorio HDN1, al Punto de Acceso de Interceptación IAP/HSS.

- Un usuario accede al Servidor de Aplicaciones AS desde un ordenador PC a través de Redes Internet IN. Él envía una petición para activar el desvío de llamadas.

- El Servidor de Aplicaciones AS comunica con la base de datos HSS por medio del protocolo LDAP. El Servidor de Aplicaciones AS proporciona el nombre del objeto de directorio HDN1.

- El nombre de directorio de HSS HDN1 proporcionado se identifica por el IAP/HSS como un objetivo interceptado.

- Los parámetros de la IRI de nombre de directorio de HSS, es decir HDN1, el Protocolo de Acceso de HSS, es decir la LDAP y Operación HSS, es decir acceder al HDN1 y activar el desvío de llamadas al número 12345, se envían como Información Relacionada con la Interceptación IRI desde el IAP a la Función de Entrega DF2 a

través del interfaz X2.

-La IRI se envía desde la DF2 a la LEA a través del interfaz H2.

Otros pasos son posibles. Por ejemplo pudiera haber un paso de identificación del usuario. El usuario no tiene que ser el abonado en sí mismo, cualquiera podría acceder a la base de datos y cambiar un perfil de usuario. Los pasos anteriores también podrían venir en otro orden. Por ejemplo es flexible en qué paso el IAP enviará la IRI a la DF2.

El usuario accede al Servidor de Aplicaciones AS desde un PC. Cualquier dispositivo que podría acceder a un AS podría ser usado, otro ejemplo es un móvil WAP WM.

El acceso al Servidor de Aplicaciones AS es en este ejemplo a través de Redes Internet. Cualquier tipo de acceso al AS podría ser posible por supuesto.

El objeto de directorio HDN1 almacena en este ejemplo los datos de usuario para un abonado. Cualquier tipo de datos se podría almacenar por supuesto en el HDN1.

En el caso de los datos relacionados con un abonado, la suscripción podría ser de cualquier tipo, por ejemplo datos o telefonía. Esta realización de la invención tiene la activación del desvío de llamadas como un ejemplo, pero por supuesto cualesquiera servicios o acceso a los datos en el HDN1 será posible de interceptar. Ejemplos de comunicación con una base de datos que se podría interceptar son la activación o desactivación, suscribir o dar de baja y la interrogación de cualquier tipo de servicio o suscripción. Los cambios del perfil de los usuarios por ejemplo el cambio de dirección o los cambios del método de facturación son otros ejemplos de datos que podrían ser interceptados.

La base de datos, es decir el HSS, se podría situar y alojar en cualquier sitio en la red. El HSS es por supuesto un ejemplo de una base de datos. Cualquier base de datos conectada a la red sería posible. Una base de datos no necesita un servidor dedicado pero se podría alojar por cualquier nodo en la red. Ese nodo será entonces el Punto de Acceso de Interceptación IAP.

El LDAP es un ejemplo de protocolo posible a usar para el acceso al objeto de directorio en el HSS. Otro ejemplo es Diámetro-Sh. En el caso de uso del LDAP como el Protocolo de Acceso al HSS el Nombre de Directorio de HSS corresponde al Nombre de Directorio de LDAP. La Operación HSS se codificará como el Mensaje LDAP como se especifica en el LDAP, RFC 2251. Ejemplos de operaciones son bindRequest y bindRespons. En el caso de uso de Diámetro-SH como el Protocolo de Acceso al HSS, la Operación HSS se codificará como Comandos como se especifica en la TS 29.329 V6.1.0. Ejemplos son la Petición de Datos de Usuario y la Respuesta de Datos de Usuario.

Los parámetros en el informe de la IRI mencionados anteriormente son solamente ejemplos y son posibles otros parámetros. El tiempo y los datos de la operación son otros ejemplos de parámetros de la IRI. Si el acceso al HDN1 falla, se podría enviar una Razón del Fallo de Acceso desde el IAP a través de la DF2 a la LEA. Si se usa un código de acceso, ese código se podría enviar también como la IRI. Tampoco es necesario incluir todos los eventos mencionados en el método anterior, solo una IRI podría ser suficiente.

La figura 3 revela un diagrama de flujo en el cual se muestran algunos pasos más importantes. El diagrama de flujo tiene que ser leído junto con las figuras mostradas antes. El diagrama de flujo comprende los pasos siguientes:

- El objeto de Directorio HDN1 se asocia a un Punto de Acceso de Interceptación. Un bloque 101 revela este paso en la figura 3.

- La Agencia Policial LEA envía una petición al punto de acceso de Interceptación, para activar la interceptación del objeto de directorio HDN1. Un bloque 102 revela este paso en la figura 3.

- El usuario accede al objeto de directorio HDN1. Un bloque 103 revela este paso en la figura 3.

- La información relacionada con el acceso y uso del HDN1 se envía desde el IAP a la LEA. Un bloque 104 revela este paso en la figura 3.

La invención no se limita por supuesto a las realizaciones anteriormente descritas y mostradas en los dibujos sino que se puede modificar dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para generar información relacionada con el acceso y el uso de un objeto de directorio (HDN1) en una base de datos (HSS) en un sistema de comunicación, cuyo sistema se equipa con la base de datos (HSS) y un objeto de directorio (HDN1) y cuyo sistema se configura para proporcionar a una Unidad de Configuración de Interceptación (ICU) la información (IRI) recogida a partir de un punto de acceso de Interceptación (HSS; IAP) por el cual el punto de acceso de Interceptación (HSS; IAP) se asocia con el objeto de directorio (HDN1), cuyo método comprende los siguientes pasos:

- recibir en el punto de acceso de Interceptación (HSS; IAP) una petición para monitorizar el objeto de directorio (HDN1),

- detección de uso del objeto de directorio en el Punto de Acceso de Interceptación (HSS; IAP),

- entregar la información (IRI) relacionada con dicho uso, desde el Punto de Acceso de Interceptación (HSS; IAP) a la Unidad de Configuración de Interceptación (ICU).

2. Un método para generar información (IRI) de acuerdo con la reivindicación 1 por el cual la Unidad de Configuración de Interceptación (ICU) comprende una Agencia Policial (LEA) adjunta a una Función de Administración (ADMF), cuyo método comprende los siguientes pasos adicionales:

- enviar desde la Agencia Policial (LEA) a la Función de Administración (ADMF), la petición para monitorizar el objeto de directorio (HDN1),

- enviar la petición de la Función de Administración (ADMF) al Punto de Acceso de Interceptación (HSS; IAP).

3. Un método para generar información (IRI) de acuerdo con cualquiera de las reivindicaciones 1 a 2 por el cual el protocolo usado para comunicar con el objeto de directorio (HDN1) es al menos uno de los siguientes:

- El Protocolo Ligero de Acceso a Directorios LDAP,

- El interfaz Sh en base al protocolo de Diámetro DSH.

4. Un método para generar información (IRI) de acuerdo con cualquiera de las reivindicaciones 1 a 3 por el cual la información entregada desde el Punto de Acceso de Interceptación (IAP) a la Unidad de Configuración de Interceptación (ICU) comprende al menos uno de los siguientes datos:

- El protocolo usado para acceder a la base de datos,

- La operación hacia la base de datos,

- El nombre de la base de datos,

- El nombre del objeto de directorio.

5. Un método para generar información (IRI) de acuerdo con cualquiera de las reivindicaciones 1 a 4 por el cual el objeto de directorio comprende los datos de usuario para un servicio de telecomunicación.

6. Un método para generar información (IRI) de acuerdo con cualquiera de las reivindicaciones 1 a 5 por el cual el objeto de directorio (HDN1) se almacena en un Servidor Local de Abonado (HSS).

7. Un método para generar información (IRI) de acuerdo con cualquiera de las reivindicaciones 1 a 6 por el cual el sistema de comunicación además comprende un servidor de aplicación (AS) y se accede al objeto de directorio a través de dicho servidor de aplicaciones (AS).

8. Un método para generar información (IRI) de acuerdo con la reivindicación 7 por el cual se accede al servidor de aplicaciones (AS) a través de Redes Internet (IN).

9. Una adaptación que comprende un punto de acceso de Interceptación para generar información relacionada con el acceso y uso de un objeto de directorio (HDN1) en una base de datos (HSS) en un sistema de comunicación, cuyo sistema se equipa con la base de datos (HSS) y un objeto de directorio (HDN1) y cuyo sistema se configura para proporcionar a una Unidad de Configuración de Interceptación (ICU) la información (IRI) recogida a partir del punto de acceso de Interceptación (HSS; IAP) por el cual el punto de acceso de Interceptación (HSS; IAP) se asocia al objeto de directorio (HDN1), cuya adaptación además comprende:

- los medios para recibir en el punto de acceso de Interceptación (HSS; IAP) una petición para monitorizar el objeto de directorio (HDN1),

- los medios para la detección del uso del objeto de directorio en el Punto de Acceso de Interceptación (HSS; IAP),

- los medios para la entrega de información (IRI) relacionada con dicho uso, desde el Punto de Acceso de Interceptación (HSS; IAP) a la Unidad de Configuración de Interceptación (ICU);

10. Una adaptación para generar información de acuerdo con la reivindicación 9 por la cual la Unidad de Configuración de Interceptación (ICU) comprende una Agencia Policial (LEA) adjunta a una Función de Administración (ADMF), cuya adaptación comprende:

- los medios para enviar desde la Agencia Policial (LEA) a la Función de Administración (ADMF), la petición para monitorizar el objeto de directorio (HDN1),

- los medios enviar la petición desde la Función de Administración (ADMF) al Punto de Acceso de Interceptación (IAP; HSS)

11. Una adaptación para generar información (IRI) de acuerdo con cualquiera de las reivindicaciones 9 a 10 adaptada de manera que el protocolo usado para comunicar con el objeto de directorio (HDN1) es al menos uno de los siguientes:

- El Protocolo Ligero de Acceso a Directorios LDAP,

- El interfaz Sh en base al protocolo de Diámetro DSH.

12. Una adaptación para generar información (IRI) de acuerdo con cualquiera de las reivindicaciones 9 a 11 por la cual el sistema de comunicación además comprende un servidor de aplicaciones (AS) y ese citado servidor de aplicaciones (AS) comprende medios adaptados para acceder al objeto de directorio (HDN1).

13. Una adaptación para generar información (IRI) de acuerdo con la reivindicación 12 por la cual el servidor de aplicaciones (AS) comprende medios adaptados para ser accedidos a través de Redes Internet (IN).

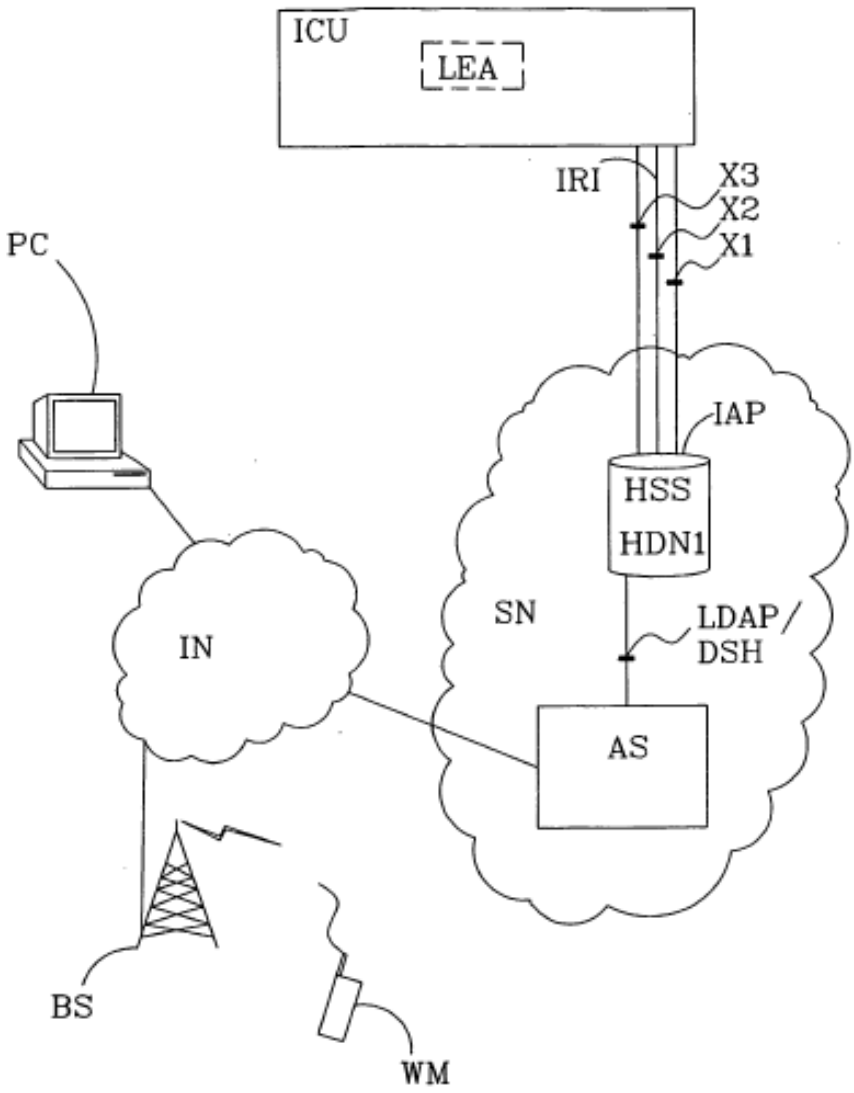

Fig. 1

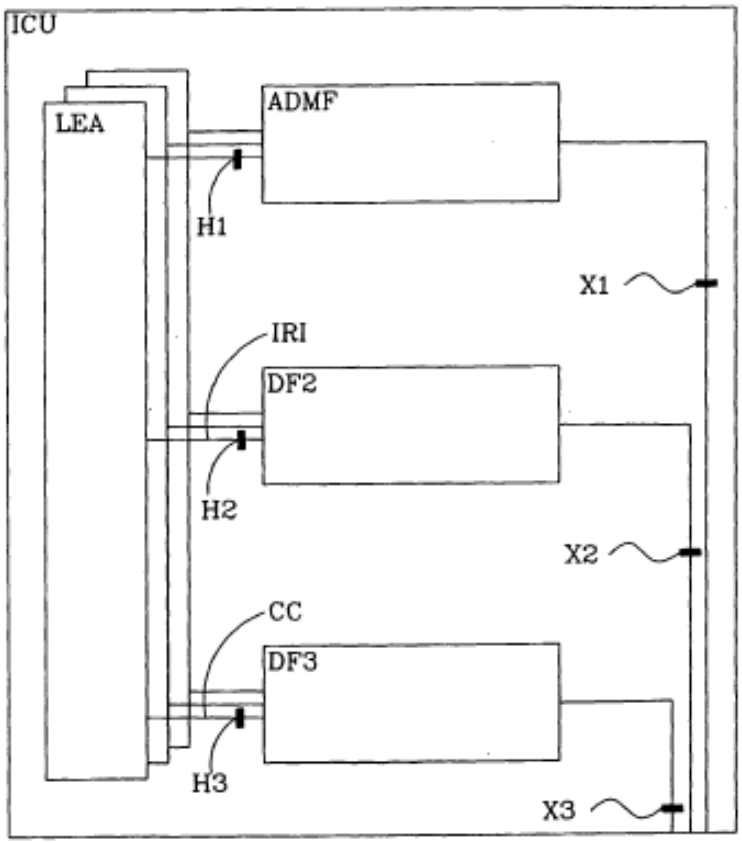

Fig. 2

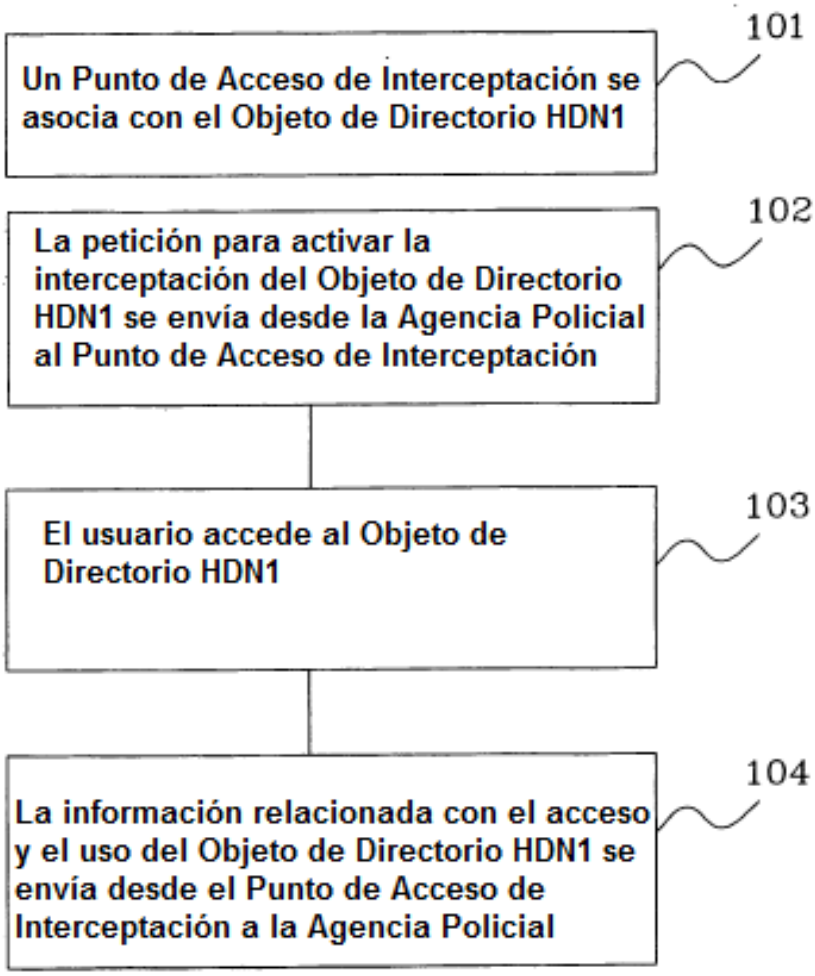
101
Un Punto de Acceso de Interceptación se asocia con el Objeto de Directorio HDN1
102
La petición para activar la interceptación del Objeto de Directorio HDN1 se envía desde la Agencia Policial al Punto de Acceso de Interceptación
103
El usuario accede al Objeto de Directorio HDN1
104
La información relacionada con el acceso y el uso del Objeto de Directorio HDN1 se envía desde el Punto de Acceso de Interceptación a la Agencia Policial

Fig. 3