(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 200**

(51) Int. CI.:
***H04L 12/14*** (2006.01)
***H04W 4/24*** (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09003938 .9**
(96) Fecha de presentación: **19.03.2009**
(97) Número de publicación de la solicitud: **2124384**
(97) Fecha de publicación de la solicitud: **25.11.2009**

(54) Título: **Procedimiento para el reconocimiento de paquetes de datos específicos de función**

(30) Prioridad:
**23.05.2008 DE 102008024796**

(45) Fecha de publicación de la mención BOPI:
**02.07.2012**

(45) Fecha de la publicación del folleto de la patente:
**02.07.2012**

(73) Titular/es:
**DEUTSCHE TELEKOM AG**
**FRIEDRICH-EBERT-ALLEE 140**
**53113 BONN, DE**

(72) Inventor/es:
**Hasemann, Jörg-Micheal**

(74) Agente/Representante:
**CARBONELL CALLICO, Josep**

## DESCRIPCIÓN

Procedimiento para el reconocimiento de paquetes de datos específicos de función

La presente invención se refiere a un procedimiento para el reconocimiento de paquetes de datos específicos de función, en especial con el objetivo de la posterior facturación, siendo los paquetes de datos generados por un terminal emisor y enviados a través de una red de líneas de datos, en especial por Internet, a un terminal receptor, presentando los paquetes de datos una cabecera ("header") y un área de datos ("payload"), teniendo los paquetes de datos asignados una funcionalidad específica, en especial un servicio particular, y siendo generados por una función adecuada, realizada en el terminal emisor. Además, la invención se refiere a un dispositivo para llevar a cabo este procedimiento.

Para el "billing", es decir la facturación de servicios de telecomunicación, se conocen diferentes modelos: Hay modelos que están basados en la comunicación ("session") en los que se factura la comunicación de una de las partes, normalmente de la parte llamante. Pero a veces, la comunicación se factura a la parte llamada como es el caso, por ejemplo, de los números "0800" conocidos en Alemania. En algunos casos aislados incluso existe la posibilidad, véase "peterzahlt.de", de que una tercera parte corre con los gastos de la comunicación. La financiación se realiza entonces especialmente a través de inserciones de publicidad.

Desde hace algún tiempo se conoce también los denominados modelos "de tarifa plana", en los que la parte llamante abona una suma global de acuerdo con un contrato firmado con el proveedor que cubre todos los servicios de telecomunicaciones salientes que pueden utilizar, además de la red telefónica, también Internet.

Además, se conocen modelos que dependen del volumen en los que la facturación se realiza basándose en el volumen de datos transferidos. Algo similar se puede decir para los modelos en los que la facturación se realiza basándose en la utilización de un formato de datos específico, es decir en un modo de transmisión determinado como los SMS y MMS, siendo esta facturación independiente del volumen de datos transferidos.

Sin embargo, los modelos de facturación conocidos actualmente están limitados en sus posibilidades de tarificación de prestaciones o servicios específicos. En especial para el cliente, resulta a veces difícil poder evaluar cuánto volumen de datos requiere un servicio determinado y cuánto cuesta realmente la utilización del servicio. Esta incertidumbre afecta precisamente la atractividad de los servicios móviles presuntamente costosos. Éstos se siguen aceptando sólo con reservas. Una facturación más transparente aumentaría la aceptación, especialmente de estos servicios móviles. Sin embargo, una condición para la facturación basada en el servicio es que el proveedor reconozca primero la utilización del servicio por el cliente.

El reconocimiento de la utilización es sencillo para el operador de red en aquellos casos en los que el servicio se proporciona por el lado de la red, es decir especialmente por el mismo operador de red. En este caso, el tráfico de datos sólo ha de ser examinado referente a la medida en que la dirección IP del servidor es utilizada como dirección de destino con tráfico de datos entrante o como dirección de origen con tráfico de datos saliente. Igual de fácil resulta el reconocimiento también, cuando se utiliza una infraestructura técnica especial para la utilización del servicio, tal como es el caso, por ejemplo, de los SMS y MMS. Sin embargo, resulta difícil en aquellos casos en los que el servicio se pone a disposición en un terminal individual. Un ejemplo para esta aplicación que se realiza substancialmente sin infraestructura del lado de la red y que utiliza la red sólo para la transmisión es "skype.com" donde se ha de descargar el correspondiente programa en el terminal antes de utilizar el servicio.

Una posibilidad de reconocer el tráfico de datos generado por estos servicios la proporcionaría el "Protocolo de Iniciación de Sesión" (Session Initiation Protocol, SIP) mediante el correspondiente "Protocolo de Descripción de Sesión" (Session Description Protocol, SDP), según RFC 3261. En este caso, se describe el tipo de sesión en el SDP. Pero si se utiliza un tipo de sesión "barato" referente a los volúmenes de datos, por ejemplo el "videostreaming", no se podrá asegurar que este servicio realmente sea utilizado en los terminales en cuestión. Puede ocurrir perfectamente que el "videostreaming" sea simulado por los terminales y que en realidad son servicios totalmente diferentes los que aprovechan para sí este "modo barato".

Además, resultan problemáticas las marcaciones de servicios basadas en SIP ya que las sesiones de SIP están formadas generalmente por el tráfico de datos de señalización y el tráfico de datos de transporte. Esto significa que dentro de la red se han de hacer coincidir eventuales marcaciones de servicio en la señalización SIP con los correspondientes tráficos de datos de transporte. Esto conlleva un considerable gasto técnico. Además, un marcado de servicio basado en SIP va ligado a servicios basados en SIP.

El documento "Policy and charging control architecture" ("Políticas y arquitectura de control de cargas") 3GPP TS23.203V8.0.0 (2007-12) describe filtros o identificadores antepuestos en el lado de red, entre otros, que asocian en una red de telefonía móvil los paquetes de datos enviados en la red a un servicio de datos específico por medio de la cabecera que contiene la dirección.

En el documento "Telecommunication management; Charging management; Charging architecture and principles"

3GPP TS 32.240 V8.2.0 (2008-03) se describe un estándar para el desarrollo de sistemas de pago en redes de telefonía móvil.

Del documento EP 1 746 772 A1 se desprende un procedimiento y un sistema para la tarificación de aplicaciones y/o el tráfico de datos asociado a las mismas en un sistema de comunicación por radio, en el que hay una función antepuesta en el lado de la red.

El documento WO 2005/004390 A1 se refiere a un procedimiento para la tarificación de datos de tráfico con la ayuda de clases de IP. Los datos de tráfico se marcan de acuerdo con una norma de asignación como pertenecientes a una clase de dirección IP. Una unidad de red a lo largo de la ruta de envío de los datos de tráfico evalúa los datos de tráfico en cuanto a su clase de IP para su tarificación, y transmite el resultado de la evaluación a otra unidad de red.

El objetivo de la presente invención consiste en dar transparencia al usuario y facilitar al operador de red de modo sencillo y seguro la tramitación a través de su red también de aquellos servicios que se inician en terminales y utilizan la estructura de red solamente para la transferencia de datos. El control ha de servir especialmente para los fines de la posterior facturación. Además, la invención también tiene el objetivo de proponer un sistema para llevar a cabo el procedimiento.

Estos objetivos se consiguen mediante el procedimiento con las características de la reivindicación 1 y el sistema según la reivindicación 8. Las realizaciones ventajosas se indican en las correspondientes reivindicaciones dependientes.

La idea fundamental de la invención consiste en el hecho de que los paquetes de datos son dotados en el terminal emisor de un marcado asimismo generado por el terminal, por medio del cual cada paquete de datos puede ser asignado a un determinado servicio mediante una función filtrante (“función de cargo por servicio”) dispuesta en la red de líneas de datos. Un marcado de este tipo se lleva a cabo por una función adecuada, instalada en el terminal, sin que haya pérdidas en el contenido de la información. Esa función puede ser cargada (“upload”) en el terminal del cliente por el operador de red o bien el cliente se la puede descargar (“download”) de la red. El marcado puede estar formado por una firma que se adjunta al paquete de datos. De acuerdo con la idea fundamental de la invención, los flujos de datos son dotados del marcado específico para cada servicio sin modificar la información de cabecera de los paquetes de datos individuales, pudiendo ser adaptada adecuadamente la suma de comprobación.

Para este tipo de marcado se pueden utilizar procedimientos de firma electrónica conocidos por el estado de la técnica, por ejemplo según el principio de clave pública (Public Key). Como marcado, se aplica de esta manera una firma electrónica que se sirve especialmente de claves privadas y públicas. Por medio de los flujos de datos marcados, el operador de red puede reconocer la utilización de servicios que se han generado fuera de su acceso, pero que utilizan su red. La invención consiste, por lo tanto, de cierta manera en un marcado o encriptación específico para cada servicio en la que la clave es, en especial, específica de la aplicación.

Resulta ventajoso que la firma se extienda a lo largo de toda el área de datos (Payload) o, como mínimo, a lo largo de partes esenciales de la misma. También puede extenderse a través de otras informaciones que complementan el área de datos, tal como la identificación del usuario, el ID del terminal y/o similares.

Una ventaja esencial es el reconocimiento específico del servicio y la posibilidad de realizar la correspondiente facturación o también el descuento. De esta manera, resultan ventajas esenciales con respecto a procedimientos que se refieren, por ejemplo, a la descripción de servicio descrita anteriormente en el marco de SIP/SDP. Otra ventaja esencial consiste en el reconocimiento de servicio a nivel del protocolo de Internet (“nivel de IP”). De esta manera, el modo de proceder, según la invención, puede ser aplicado a todos los protocolos que están basados en IP, de manera que la facturación específica de servicio es posible para aplicaciones que están basadas en SIP, http, RTP o IP.

Del reconocimiento resultan, además, otras ventajas. Durante un “streaming” a través de un terminal móvil se puede, por ejemplo, aumentar el ancho de banda o los parámetros de QoS de forma específica para cada servicio. Desde el punto de vista de una empresa de telecomunicaciones resulta ventajoso que a partir de ahora se pueden controlar y facturar también los servicios generados en terminales. De esta manera, las aplicaciones mencionadas tal como Skype se vuelven valiosas también para las empresas de telecomunicaciones con infraestructura de red. En este caso, también es posible que la red o el proveedor del servicio adquiera mejores condiciones de transmisión del operador de red para su servicio adecuadamente marcado, especialmente un ancho de banda más amplio o garantizado, menos “jitter”, es decir menos cambios bruscos e indeseados de la característica de señal y/o reducidos tiempos de latencia.

Además, el modo de proceder, según la invención, facilita el desplazamiento de la generación del servicio a terminales, en especial móviles, cada vez más pequeños y más rápidos. Esto ocurre porque con el procedimiento de la invención el proveedor del servicio y el proveedor de la red de transporte tienen a disposición un medio con el que se pueden reconocer servicios generados en el lado del terminal. Debido a que ahora, por un lado, se pueden facturar los servicios que se habían utilizado hasta el momento de forma gratuita y que, por otro lado, se puede

ofrecer un compromiso de calidad de servicio específico del servicio para la transmisión, se produce una situación win-win para el operador de red y para el proveedor de servicios implementados en el lado del terminal. El modo de proceder, según la invención, ofrece al cliente una facturación justa, transparente y basada en el volumen de utilización referida al servicio.

La invención también hace posible la vía inversa. Las funciones instaladas por los operadores de red en los terminales de sus clientes hacen posible que un determinado tipo de transferencia de datos no sea recogido por la facturación. Además, también se pueden enlazar funciones que miden continuamente los parámetros de calidad de servicio de la red o determinan la ubicación actual y transmiten estos parámetros al operador de red. En total, la flexibilidad queda mejorada con respecto a una facturación basada en las direcciones de origen y de destino por el hecho de que las direcciones IP pueden ser modificadas por los servicios, sin que ello influya sobre la facturación.

Además, se puede garantizar una protección contra la utilización de la aplicación en redes ajenas. Finalmente, las aplicaciones modificadas de acuerdo con el procedimiento mostrado aquí no se pueden utilizar sin más en redes ajenas, a no ser que la red ajena ponga a disposición la aplicación y las claves. Desde el punto de vista del operador de red las aplicaciones están acopladas a la red en el lado del cliente.

El modo de proceder mostrado es fácilmente escalable y se deja representar como componente en elementos de redes de acceso, por ejemplo, como parte de un “controlador de frontera de sesión” (Session Border Controller).

A continuación, se explicará la invención con más detalle haciendo referencia a las figuras 1 y 2. Éstas muestran:

Figura 1 un gráfico de la “función de desarrollo de servicios” y

Figura 2 un gráfico del desarrollo del procedimiento, según la invención.

Los sistemas para llevar a cabo el procedimiento, según la invención, presentan especialmente los siguientes componentes: Primero se prevén los terminales necesarios para la utilización del servicio que están conectados a la red del proveedor de telecomunicaciones. Los terminales tienen instaladas las funciones que prestan el servicio. En la misma red está dispuesta una función de cargo por servicio (Service Charge Function, SCF) como función de red que reconoce y registra el tráfico de datos marcado específicamente. Además, en la red está dispuesta una función de desarrollo del servicio (Service Deployment Function, SDF) con la que se pueden configurar las funciones y cargarlas e instalarlas en los terminales como “bundles” o fajos. El procedimiento, según la invención, puede ser dividido en tres etapas:

Etapa A: Preparación de las funciones y carga (“Deployment”)

La preparación de las funciones y su “deployment” o desarrollo en el terminal se llevan a cabo por la función de desarrollo de servicio SDS 1 mostrada en la figura 1: Primero la empresa de telecomunicaciones edita una clave privada 2, necesaria para crear la firma, para el transporte de datos y la entrega junto con la aplicación. Conjuntamente con el código de servicio (Service Code) 3 codificado, por ejemplo en Java, se genera un código fuente (Source Code) 4 parametrizado con la clave destinada al transporte de datos. La clave es parte integral del paquete de instalación que se instala en el terminal. Todos los datos que saldrán posteriormente de la aplicación a las redes de la empresa de telecomunicaciones son firmadas por el terminal con esta clave. La clave privada, así como el código de la aplicación pueden ser ofuscados 5 con las medidas adecuadas tales como, por ejemplo, mediante compilación o con ofuscadores.

Para asegurar la integridad de la aplicación y de la clave del transporte de datos 2 la empresa de telecomunicaciones firma los paquetes de instalación con una clave adecuada 6, siendo ésta diferente de la clave 2 para el transporte de datos. Esta firma del paquete de instalación 7 garantiza la originalidad de la aplicación e impide que intrusos (troyanos) puedan robar la identidad de la aplicación.

Mediante mecanismos de gestión remota de dispositivos (Remote Device Management) se instalan los paquetes de instalación 7 en el terminal 9 especificado por el juego de datos 8 en un entorno de ejecución 11 adecuadamente seguro, siendo señaladas las funciones instaladas con el numeral 10. Adicionalmente, se modifica la clave privada en intervalos regulares y se actualiza mediante actualización remota en los terminales afectados, repitiéndose las etapas representadas.

Las claves utilizadas pueden ser depositadas para su posterior verificación durante el transporte de datos por la SCF en bancos de datos adecuados, por ejemplo, de forma global en un banco de datos 12 para claves válidas o de forma específica para cada usuario y/o terminal en un banco de datos de perfil de usuario 13.

Etapa B: Marcado de servicio

En la figura 2 se muestra el terminal designado 9, con el entorno de ejecución seguro y la funcionalidad, según la invención, de las funciones instaladas 10. Con la funcionalidad 10, según la invención, se codifica todo el tráfico

saliente, generado por una aplicación (servicio) que se ejecuta en el terminal 9, a nivel del área de datos del paquete. A tal efecto, un paquete de datos 14 generado inicialmente por la aplicación está compuesto de una cabecera ("header") 15 y un área de datos ("payload") 16. En la cabecera 15 están depositadas especialmente la dirección de destino del paquete de datos así como las informaciones acerca de la integridad del paquete de datos. Durante el marcado, según la invención, cada paquete de datos 14 es transformado en un nuevo paquete de datos 17:

A través del paquete de datos original 14 se crea una firma 19 con la ayuda de la clave 18 que corresponde a la clave 2, y con esta firma se genera una nueva área de datos 20. Ésta resulta de la cabecera original 15', el área de datos original 16' y por anteponer la firma 19. Para la creación de la firma se utilizan procedimientos habituales utilizando sistemas asimétricos de clave pública. En la próxima etapa se forma una nueva cabecera 21 que resulta de la cabecera original 15, siendo la suma de comprobación de la cabecera 21 adaptada a la nueva situación. Exceptuando la dirección de destino que es adaptada con el fin de desviar los paquetes de datos 17 a la dirección de la función de cargo por servicio (SCF) 22, todo lo demás queda igual que antes.

En el caso de que la longitud total del paquete de datos 17 sobrepase la longitud máxima, éste puede ser fragmentado y el área de datos puede ser distribuido en dos paquetes de datos. En esta forma se enviará el paquete de datos 17 de dirección a la dirección de destino, señalando esta dirección de destino a la SCF, tal como se ha descrito anteriormente.

Etapa C: Identificación y demarcación

En la etapa B se ha modificado la dirección de destino del paquete de datos 17 a la de la SCF 22, de manera que es dirigido allí a través de la red 23. La SCF 22 verifica mediante su clave pública la autenticidad del paquete de datos. Si la verificación se realiza con éxito, se comunica este hecho a los sistemas dispuestos detrás 24 que gestionan, por ejemplo, la facturación de manera que se puede llevar a cabo una tarificación correcta en función del servicio. A tal efecto, se parte primero del caso de que ambos participantes en la comunicación están conectados directamente a la red 23 de la empresa de telecomunicaciones. De esta manera, se tienen en cuenta todos los participantes, uno para el tráfico de datos salientes, el otro para los entrantes.

Si la verificación no se lleva a cabo con éxito, el paquete de datos 17 será descartado. En su caso, la funcionalidad 24 puede realizar una "detección de fraude" (Fraud Detection) para investigar la causa, por ejemplo un intento de piratería. Dado que las claves son cambiadas regularmente, la SCF 22 puede verificar por medio del banco de datos 12 si, eventualmente, las claves públicas utilizadas son obsoletas. También se puede llevar a cabo una comparación con el banco de datos de perfiles de usuarios 13. Si no se puede enmendar el error por medio de las verificaciones, el paquete de datos será descartado.

Una vez identificado el paquete de datos 17 se realiza su demarcación deshaciendo los pasos que se han realizado en la etapa B. Esto significa que se restablece el paquete de datos original 14 con la cabecera original 15, el área de datos original 16 y la correspondiente dirección original, y el mismo es enviado a través de la red 25 al destinatario 26 al que estaba destinado inicialmente. Sin el "desvío", según la invención, éste hubiera sido contactado directamente por la vía 27 a través de la red no mostrada.

**REIVINDICACIONES**

1. Procedimiento para el reconocimiento de paquetes de datos específicos de función, que son generados por un terminal emisor y enviados a través de una red de líneas de datos a un terminal receptor, presentando los paquetes de datos una cabecera (“header”) y un área de datos (“payload”), teniendo los paquetes de datos asignados un servicio especial y siendo los mismos generados por una función adecuada, realizada en el terminal emisor, en el que se adjunta a los paquetes de datos un marcado específico generado en el terminal por medio de la cual una función filtrante (“función de carga por servicio”) dispuesta en la red de líneas de datos reconoce los paquetes de datos marcados y los asigna a la funcionalidad específica, sin que haya pérdidas en el contenido de información, **caracterizado porque** el marcado es aplicado por una función cargada en el terminal, y **porque** como marcado se aplica una firma electrónica específica para el servicio.

2. Procedimiento, según la reivindicación 1, **caracterizado porque** la carga de la función la lleva a cabo el operador de la red.

3. Procedimiento, según la reivindicación 1 ó 2, **caracterizado porque** la firma se sirve de claves privadas y públicas.

4. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado porque** durante el marcado se escribe una nueva dirección en la cabecera de los paquetes de datos mediante la cual se desvían los mismos a la función de cargo por servicio (“SCF”).

5. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado porque** dentro de la SCF se elimina el marcado y los paquetes de datos adquieren otra vez su forma inicial.

6. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado porque** el filtrado por SCF se utiliza para los fines de la facturación, en especial de la utilización de la red.

7. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado porque** los paquetes de datos son enviados de acuerdo con un protocolo basado en IP, siendo posible en especial una facturación específica de servicio para aplicaciones que están basadas en SIP, http, RTP o IP.

8. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado porque** durante el reconocimiento de los paquetes de datos marcados se inicia un aumento del ancho de banda o de los parámetros QoS.

9. Sistema que lleva a cabo el procedimiento, según una de las reivindicaciones anteriores.

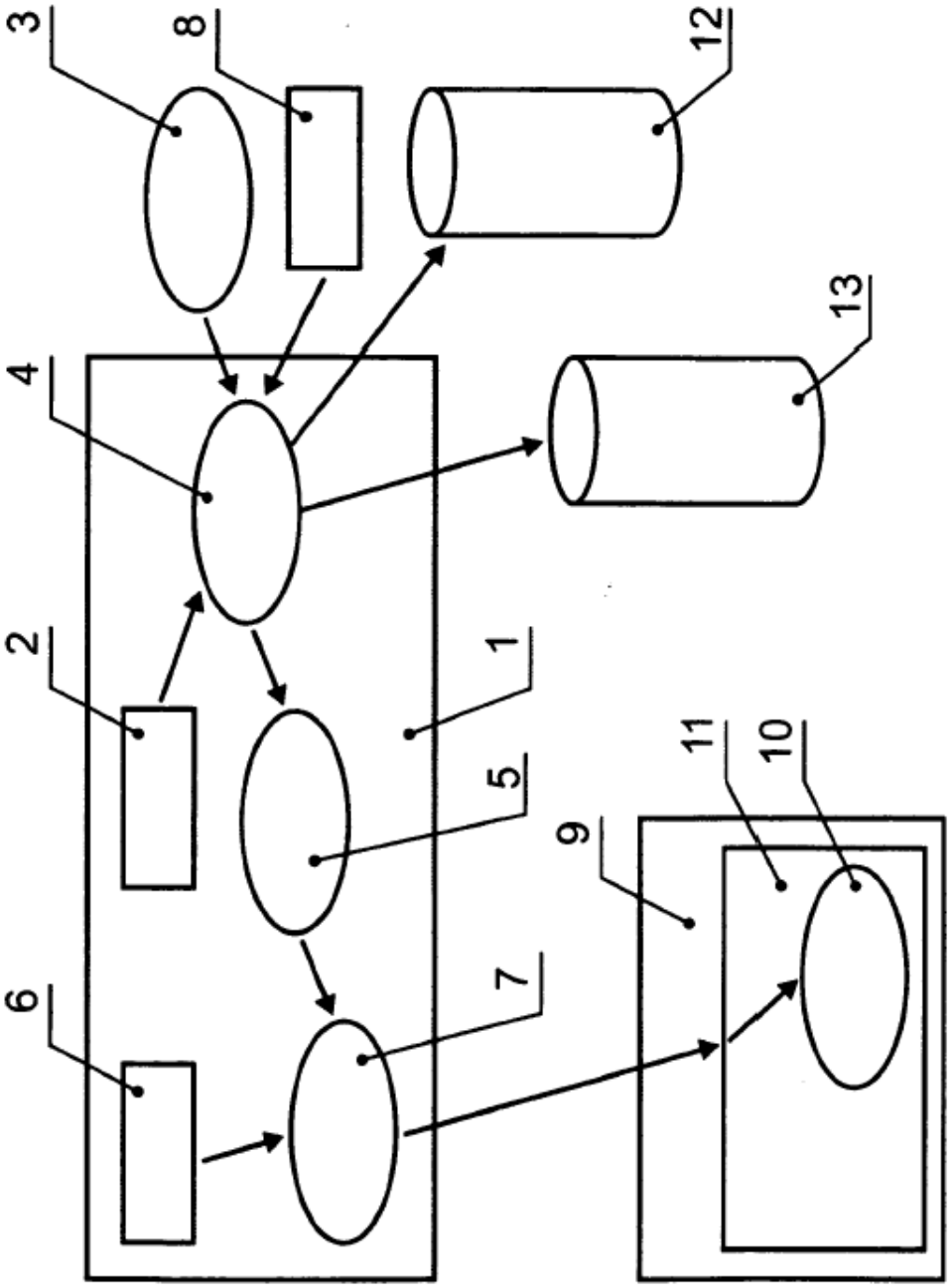


Fig. 1

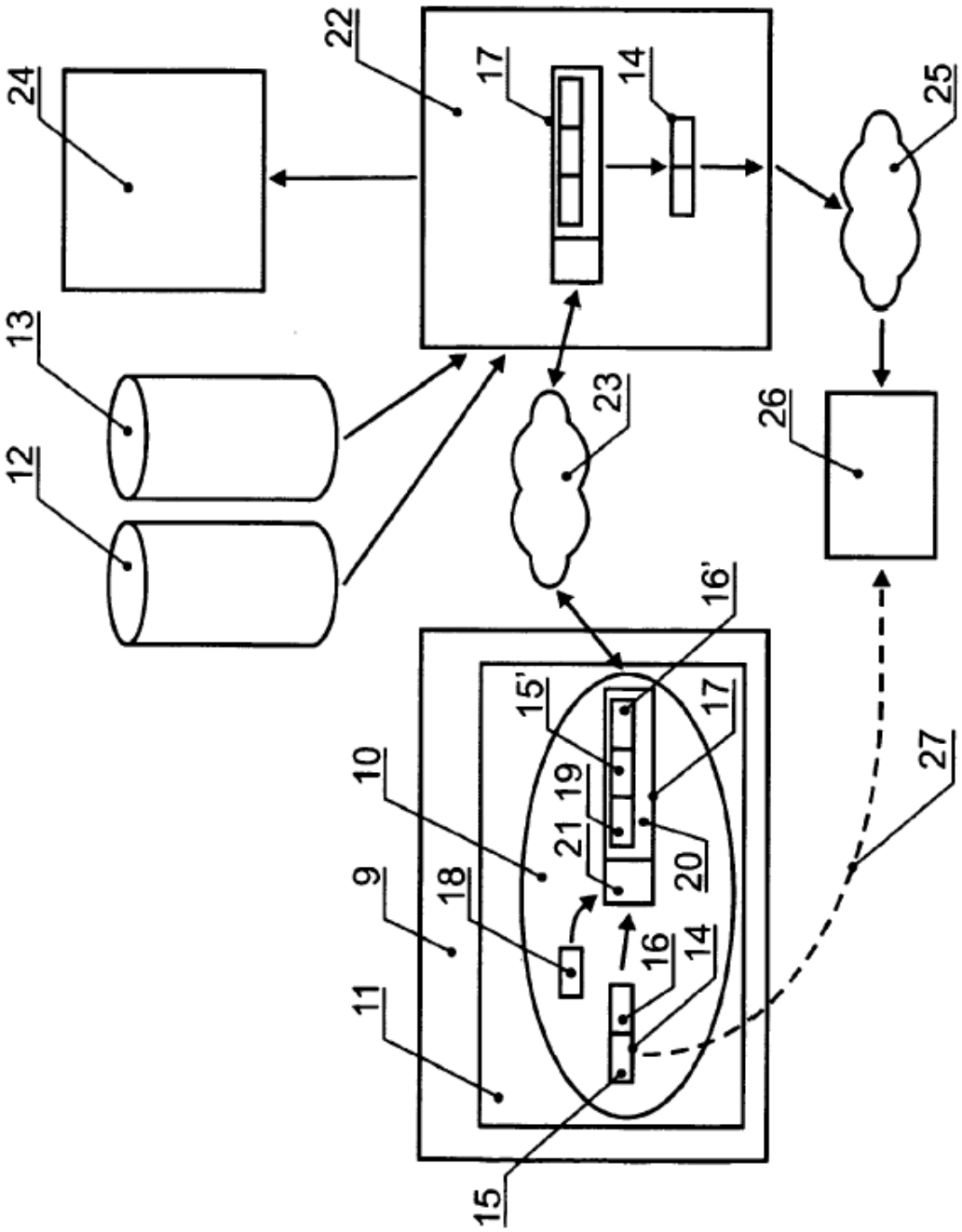


Fig. 2