(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 612 467**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.12.2011 E 11194389 (0)**

(97) Fecha y número de publicación de la concesión europea: **09.11.2016 EP 2466849**

(54) Título: **Distribución selectiva de un flujo multidifusión**

(30) Prioridad:

20.12.2010 FR 1060848

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.05.2017

(73) Titular/es:

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

(72) Inventor/es:

VIVOLO, OLIVIER y
FONTAINE, NOËL

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Distribución selectiva de un flujo multidifusión

La presente invención se refiere a la distribución selectiva de flujos de datos con destino a usuarios de una red de distribución de contenidos.

Es posible distribuir de manera selectiva un contenido protegido desde un control efectuado por un elemento de la red (enrutador, DSLAM ("*Digital Subscriber Line Access Multiplexer*"), etc.). El control se efectúa previamente a la distribución del contenido por el elemento situado en la red.

Por ejemplo, el control se dirige a la adecuación entre las condiciones de acceso presentes en el flujo y los derechos del usuario almacenados en una tabla del elemento de la red.

El envío del flujo está condicionado por la adecuación de informaciones extraídas de la señal por el equipo de la red y los derechos del usuario almacenados en la memoria del equipo.

Es necesario entonces tener una capacidad de almacenamiento en el equipo de la red que le permita memorizar las informaciones relativas a los derechos de los terminales conectados.

Además, los tratamientos pueden convertirse en complejos en el caso de almacenamiento local de las autorizaciones. En efecto, antes de proceder a la distribución del contenido, el equipo de la red debe ser capaz de extraer los elementos pertinentes de la señal recibida con el fin de realizar la comparación con las autorizaciones presentes.

Según otro ejemplo, el control se efectúa por un elemento de la red y se dirige a un tique obtenido desde un servidor que gestiona el acceso al servicio. En este caso, el elemento de la red y el servidor que suministran el tique comparten una misma base de datos.

Es necesario entonces establecer un enlace (o la compartición de datos) entre el sistema de informaciones (SI) comercial del operador que gestiona el servicio y los elementos de la red a cargo de efectuar el control de los datos comerciales asociados a los contenidos protegidos (pertenencia a una oferta o identificador de la oferta, validez de un tique en la base de datos, etc.).

Además, este modo de funcionamiento crea un enlace fuerte entre el SI comercial del operador del servicio y la red encargada de la distribución del contenido, mientras que se busca más frecuentemente separar la red y los servicios.

En los dos ejemplos anteriores en los que el operador del servicio no es el operador de la red, el mecanismo propuesto impone una compartición de informaciones y también la colocación de pasarelas entre los operadores.

Según otro ejemplo más, el control del acceso a Internet y de las autorizaciones de servicio se efectúa mediante el control de una solicitud transmitida por el DSLAM ("*Digital Subscriber Line Access Multiplexer*") en la dirección de un servidor que funciona según el protocolo RADIUS ("*Remote Authentication Dial-In User Service*").

En este ejemplo, es necesario que la autorización se efectúe mediante un tercer servidor (control desviado).

Además, el control necesita el añadido de un equipo externo (el servidor RADIUS).

En todos los casos, sea o no el operador del servicio el operador de la red, es necesario crear unas pasarelas complejas y costosas (porque son inexistentes muy frecuentemente) entre los frontales comerciales y los equipos que intervienen en la distribución final del contenido (DSLAM por ejemplo).

El documento EP 1 176 490 describe un sistema de distribución de contenidos cifrados a un dispositivo receptor. El sistema comprende un dispositivo de cesión de los derechos así como un distribuidor de contenido.

El documento US 2003/0217163 se refiere a un procedimiento de acceso condicional que permite atribuir un derecho de acceso a un terminal de usuario, en el que se genera una cadena de datos mediante un módulo de generación de un servidor de acceso, comprendiendo esta cadena unos datos de derecho de acceso.

El documento EP 1 610 200 describe un procedimiento de descarga desde un servidor en una red de comunicación móvil. En particular, el procedimiento se refiere a la descarga de contenidos multimedia desde el servidor hacia el equipo de usuario y permite la protección del derecho de autor asociado al contenido multimedia impidiendo la descarga sin previo acuerdo.

La invención propone unas mejoras a las soluciones existentes.

Con este fin, según un primer aspecto de la invención, se propone un procedimiento de acceso a un flujo de datos de contenido mediante un terminal de telecomunicaciones en una red de telecomunicaciones, que incluye las etapas siguientes implementadas por el terminal:

- envío de una primera solicitud con destino a una entidad de gestión de acceso a un servicio, dirigiéndose esta primera solicitud a identificar el terminal ante la entidad de gestión de acceso al servicio

- después de la identificación del terminal por la entidad de gestión de acceso al servicio, recepción de medios de autenticación proporcionados por la entidad de gestión de acceso al servicio,

- envío de una segunda solicitud con destino a una entidad de acceso, dirigiéndose esta segunda solicitud al acceso por el terminal al flujo de datos de contenido, y siendo generada esta segunda solicitud utilizando los medios de autenticación proporcionados por la entidad de gestión de acceso al servicio, y

- recepción procedente de la entidad acceso de un flujo de datos de contenido, tras una autenticación positiva del terminal ante la entidad de acceso.

Se puede así realizar la distribución selectiva de un flujo, particularmente de un flujo multidifusión, a unos usuarios debidamente autorizados e identificados sin que sea necesario establecer un enlace regular entre los equipos de la red (DSLAM) del operador de la red y el sistema de informaciones comerciales (abonados) del operador del servicio.

De ese modo se reduce el impacto del control efectuado por el equipo de la red a la verificación de una firma durante la solicitud de acceso al flujo efectuada por el terminal.

Por otro lado, ya no es necesario el enlace entre el SI comercial del operador del servicio y los equipos de la red (incluso con un equipo externo). El control puede ser del tipo “stand alone”.

Es igualmente posible limitar la configuración de los equipos de la red encargados de efectuar este control, con la inserción de una clave local previamente a la apertura del servicio.

De ese modo, el tratamiento realizado por estos equipos puede limitarse a la verificación de una firma de los parámetros transmitidos en la solicitud del terminal demandante.

De una manera general se puede distribuir selectivamente un flujo manteniendo una separación servicio/red.

Pueden insertarse fácilmente unos modos de realización en una arquitectura mono operador pero también, multi-operador.

Se ofrece igualmente un complemento a la seguridad de acceso a un flujo. Los contenidos no pueden distribuirse más que a los usuarios debidamente identificados como que son clientes del servicio.

Pueden aplicarse unos modos de realización a las distribuciones selectivas de contenidos (IPTV), principalmente en la red de fibra (FTTH) o de cobre (ADSL).

Unos modos de realización permiten ofrecer una nueva funcionalidad en una red ya existente sin impactar fuertemente en la distribución del flujo selectivo.

Unos modos de realización pueden incluir una o varias de las medidas siguientes.

La entidad de gestión de acceso al servicio determina uno o varios derechos de acceso del terminal a uno o varios flujos de datos.

La primera solicitud y/o la segunda solicitud incluyen al menos uno de entre un identificador del terminal y una dirección de red del terminal.

Los medios de autenticación incluyen una primera clave criptográfica, por ejemplo para firmar la segunda solicitud.

La entidad de acceso obtiene la primera clave criptográfica y autentica la segunda solicitud verificando la firma de la segunda solicitud por medio de la primera clave criptográfica.

La primera clave criptográfica se obtiene dinámicamente a partir de al menos uno de entre un identificador del terminal y una dirección de red del terminal.

Los medios de autenticación incluyen un certificado de autenticación que autoriza el acceso por el terminal al flujo de datos.

El certificado incluye además una duración de validez del certificado.

El certificado incluye al menos un identificador que puede verificar la entidad de acceso (por ejemplo el identificador de línea telefónica, el número de puerto sobre el que está conectada la línea telefónica a la entidad de acceso,…).

La segunda solicitud incluye el certificado.

La entidad de acceso verifica el certificado por medio de una segunda clave de autoridad de certificación.

La segunda solicitud está firmada por el terminal por medio de la tercera clave criptográfica.

La entidad de acceso autentica la segunda solicitud verificando la firma de la segunda solicitud por medio de la tercera clave criptográfica.

Según otros aspectos de la invención, se prevé:

- un programa informático que incluye unas instrucciones para la implementación de un procedimiento según el primer aspecto de la invención cuando el programa lo ejecuta un procesador;
- un soporte legible por un ordenador en el que se registra un programa informático de ese tipo;
- un terminal de telecomunicaciones para la implementación de un procedimiento según el primer aspecto de la invención.

Un terminal de ese tipo incluye:

- una unidad de comunicación configurada para enviar una primera solicitud con destino a una entidad de gestión de acceso a un servicio, dirigiéndose esta primera solicitud a identificar el terminal ante la entidad de gestión de acceso a un servicio, para recibir unos medios de autenticación proporcionados por la entidad de gestión de acceso al servicio después de la identificación del terminal por la entidad de gestión de acceso a un servicio, para enviar una segunda solicitud con destino a una entidad de acceso, dirigiéndose esta segunda solicitud al acceso por el terminal al flujo de datos de contenido, y para recibir, procedente de la entidad de acceso, un flujo de datos de contenido, tras una autenticación positiva del terminal ante la entidad de acceso, y
- una unidad de tratamiento configurada para generar la segunda solicitud utilizando los medios de autenticación proporcionados por la entidad de gestión de acceso al servicio.

Las ventajas proporcionadas por el programa informático, el soporte legible por ordenador, y el terminal, tal como se han expuesto sucintamente en el presente documento anteriormente, son idénticas al menos a aquellas mencionadas más arriba en conexión con el procedimiento según el primer aspecto.

Surgirán a otras características y ventajas de la invención con la lectura de la descripción a continuación. Esta es puramente ilustrativa y debe leerse en relación a los dibujos adjuntos en los que:

- La figura 1 ilustra un sistema general de implementación de modos de realización de la invención;
- la figura 2 es un organigrama general que representa unas etapas implementadas según un primer modo de realización;
- la figura 3 es un organigrama general que representa unas etapas implementadas según un segundo modo de realización;
- la figura 4 es un organigrama general que representa unas etapas implementadas según un tercer modo de realización; y
- la figura 5 ilustra esquemáticamente la estructura de elementos comprendidos en un sistema de estos modos de realización de la invención.

La figura 1 ilustra un sistema general de implementación de diferentes modos de realización de la invención, según un ejemplo particular de realización. Este sistema comprende:

- una entidad GAS de gestión de acceso a un servicio 11 que gestiona en este caso el acceso de los terminales 10 a un servicio de TV de transmisión de programas audiovisuales, proporcionado por un operador y eventualmente organizado en grupos de cadenas de TV,

- una base de datos de usuarios 12, conectada a la entidad GAS 11 de gestión de acceso al servicio y que almacena las informaciones relativas a los usuarios del servicio de TV proporcionadas por el operador del servicio, comprendiendo esas informaciones particularmente unos derechos de abono de los usuarios a unos programas audiovisuales eventualmente organizados en grupos de cadenas de TV,

- una entidad de acceso a unos flujos de datos de programas audiovisuales, en este caso un DSLAM 13.

- una base de datos 15 conectada a la entidad de acceso 13, y

- un terminal de usuario 10, por ejemplo un “set top box”, dicho de otra manera un decodificador receptor de TV.

Por supuesto, la entidad de gestión del servicio 11 podría proporcionar un servicio distinto a la transmisión de programas de TV.

La base de datos 15 contiene un conjunto de pares que comprende, cada uno, una clave criptográfica Ki y un conjunto que comprende uno o varios flujos de datos de programa audiovisual. Estos pares se proporcionan por el operador que gestiona el servicio de TV.

Los programas de TV se transmiten en la forma de flujos de datos a través de una red 14. La entidad acceso 13, la entidad de gestión de acceso al servicio 11 y el terminal 10 están conectados a la red 14.

Se va a describir ahora de una manera general el procedimiento de acceso por el terminal a un flujo de datos del programa audiovisual transmitido a través de la red.

El terminal 10 envía una solicitud hacia la entidad de gestión de acceso al servicio 11, para acceder al flujo de datos. La entidad GAS 11 de gestión de acceso al servicio se encarga de determinar si el terminal 10 tiene los derechos de acceso necesarios para acceder al flujo. Por ejemplo, verifica los derechos de abono del terminal. Con este fin, la entidad GAS 11 puede consultar la base de datos 12 que incluye las informaciones de las que tiene necesidad. Se realiza en este caso la hipótesis de que el terminal 10 tiene los derechos suficientes para acceder al flujo demandado.

Cuando la entidad de gestión de acceso al servicio 11 ha verificado que el terminal 10 puede acceder al flujo, le proporciona unos medios de autenticación destinados a ser utilizados a continuación para acceder al flujo deseado.

Tras la recepción de los medios de autenticación, el terminal 10 accede a la red 14 a través de la entidad de acceso, por ejemplo un DSLAM 13, utilizando los medios de autenticación que se le han proporcionado por la entidad 11 de gestión de acceso al servicio.

El DSLAM 13 autentica el terminal 10 y autoriza o no el acceso al flujo demandado, según que la autenticación sea válida o inválida. Para autenticar al terminal 10, el DSLAM 13 puede consultar una base de datos 15 que incluye las informaciones de las que tiene necesidad.

En caso de autenticación válida, el DSLAM 13 transmite el flujo de datos demandado al terminal 10.

En lo que sigue, se describen tres modos distintos de realización particulares del procedimiento de acceso a un flujo de datos por el terminal 10, según la invención.

El primer modo de realización se describe con referencia a la figura 2.

El terminal 10 envía una solicitud Solic1 hacia la entidad 11 de gestión de acceso al servicio (GAS) 11 durante la etapa S200. Esta solicitud Solic1 le permite identificarse ante la entidad de gestión de acceso al servicio 11 y, como se verá en lo que sigue, obtener unos medios de autenticación para recibir el flujo transmitido por la red 14. La solicitud Solic1 incluye unas informaciones de identificación del terminal 10 (y/o del usuario), por ejemplo un identificador del terminal (o del usuario), y una dirección IP del terminal.

La entidad 11 de gestión de acceso al servicio (GAS) recibe la solicitud Solic1. Determina a continuación durante la etapa S201, la entidad del usuario o bien a partir del identificador del terminal o bien a partir de la dirección IP del terminal.

Durante esta misma etapa S201, la entidad de gestión de acceso al servicio 11 determina a partir de la identidad del usuario los derechos del usuario sobre los diferentes flujos disponibles en la red. Por ejemplo, la entidad de gestión de acceso al servicio 11 consulta una tabla, almacenada en la base de datos; de correspondencia entre unas informaciones de identificación de usuario y/o de terminal y un conjunto de identificadores de flujo {Flux.id} autorizados al que este terminal 10 puede acceder.

La entidad de gestión de acceso al servicio 11 recupera entonces una (o varias) clave criptográfica K1 desde la base de datos 15 para el conjunto de los flujos {Flux.id} autorizados para el usuario y lo (o los) transmite al usuario durante la etapa S202.

Cuando el usuario desea acceder a una cadena particular, dicho de otra manera a un flujo de datos de audio/video particular, el terminal 10 emite, durante la etapa S204, una solicitud Solic2 al DSLAM 13 para obtener el flujo de audio/video deseado. La solicitud Solic2 se firma con la clave K1 que se asocia al flujo demandado. La firma de la solicitud Solic2 se realiza durante la etapa S203. La solicitud Solic2 incluye por ejemplo la dirección IP del terminal, la dirección IP del flujo demandado, y la firma de la solicitud.

El DSLAM 13 se configura por el operador de la red 14 con unas claves asociadas al flujo. Utiliza la clave K1 en función de la dirección IP del flujo demandado (Flux IP). Por ejemplo, el DSLAM 13 obtiene la clave en la base de datos 15 (que puede ser de hecho la misma base de datos 12), durante la etapa S205. El DSLAM verifica la firma de la solicitud Solic2 con la ayuda de esta clave durante la etapa S206.

Según ciertas alternativas, la clave a utilizar para generar la firma de la solicitud Solic2 es una clave obtenida dinámicamente a partir de la dirección IP del terminal. Según otras alternativas, se obtiene a partir de un identificador del terminal y de la clave K1. En este caso, el terminal 10 y el DSLAM 13 realizan por separado una misma operación de cálculo con el fin de determinar la clave a utilizar.

Cuando se efectúan las verificaciones, el DSLAM envía una respuesta al terminal 10 durante la etapa S207. Esta respuesta puede incluir una indicación de aceptación del acceso al flujo, o de un rechazo del acceso al flujo, según que las verificaciones efectuadas se hayan logrado o hayan fracasado.

Cuando las verificaciones se logran, el flujo se transmite por el DSLAM 13 al terminal 10 durante la etapa S208.

Se describe un segundo modo de realización particular con referencia a la figura 3.

Como en el primer modo de realización, se envía una solicitud de autenticación Solic1 que permite identificarse ante la entidad GAS de gestión de acceso al servicio 11 por parte del terminal 10 hacia la entidad de gestión de acceso al servicio 11 durante la etapa S200, y la entidad de gestión de acceso al servicio 11 efectúa unas verificaciones durante la etapa S201.

En este segundo modo de realización particular, en lugar de una clave criptográfica, la entidad de acceso al servicio 11 genera un certificado electrónico de autenticación Cert durante una etapa S302, y transmite este certificado durante la etapa S303 al terminal 10.

Por ejemplo, el certificado electrónico de autenticación Cert contiene los derechos del usuario sobre un conjunto de flujos identificados por un identificador de flujo “flux.ID” o por una dirección IP del flujo “Flux.IP” (o bien los dos) y una duración de validez. El certificado electrónico Cert se firma por la entidad de gestión de acceso al servicio 11.

Cuando el usuario del terminal 10 desea ver una cadena particular, dicho de otra manera acceder a un flujo de datos particular, el terminal 10 emite, durante la etapa S304, la solicitud Solic2 hacia el DSLAM 13 para obtener el flujo de audio/video. En este modo de realización, la solicitud Solic2 es una solicitud no firmada pero el terminal 10 inserta en ella el certificado obtenido ante la entidad GAS de gestión de acceso al servicio 11.

El DSLAM 13 verifica, durante la etapa S305, el certificado Cert y su validez y verifica que el flujo demandado (sea con Flux.ID o sea con Flux.Ip) forma correctamente parte de los flujos autorizados en el certificado Cert.

La entidad GAS de gestión de acceso al servicio 11 puede añadir en el certificado Cert o bien un identificador de la línea telefónica o bien un número de puerto en el que está conectada la línea telefónica al DSLAM. Esto permite además al DSLAM controlar de manera “física” la procedencia de la solicitud Solic2.

A continuación, el proceso continúa con las etapas S207 y S208 mencionadas anteriormente para el primer modo de realización.

Se describe un tercer modo de realización particular con referencia a la figura 4. Como en el primer modo de realización, la solicitud Solic1 se envía por parte del terminal 10 hacia la entidad GAS de gestión de acceso al servicio 11 durante la etapa S200, y la entidad GAS de gestión de acceso al servicio 11 efectúa unas verificaciones durante la etapa S201.

A continuación, la entidad de gestión de acceso al servicio 11 recupera una clave pública asociada al terminal bien interrogando la base de datos 12, o bien por extracción de la solicitud Solic1 en el caso de que el terminal haya insertado una clave pública en la solicitud Solic1.

La entidad de gestión de acceso al servicio 11 genera a continuación un certificado Cert para la clave pública del terminal 10, como se ha descrito anteriormente para el segundo modo de realización.

Cuando el usuario del terminal 10 desea ver una cadena particular (un flujo particular), el terminal 10 emite la solicitud Solic2 al DSLAM 13 para obtener el flujo de audio/video.

La solicitud Solic2 se firma por el terminal 10 durante la etapa S404 utilizando la clave privada del terminal. El certificado Cert se envía igualmente en la solicitud Solic2.

El DSLAM 13 verifica entonces:

- el certificado Cert y su validez (etapa S305),

- que la firma de la solicitud Solic2 (la clave pública para verificar Firm2 está incluida en Cert) es correcta (etapa S206), y

- que la dirección IP del flujo @Flux.IP (o bien el identificador del flujo “Flux.ID”) es una de las direcciones IP (o bien uno de los flujos) autorizados en el certificado.

La entidad de gestión de acceso al servicio 11 puede añadir en el certificado Cert o bien un identificador de la línea telefónica o bien un número de puerto en el que está conectada la línea telefónica al DSLAM. Esto permite además al DSLAM 13 controlar de manera “física” la procedencia de la solicitud Solic2.

A continuación el proceso continúa con las etapas S207 y S208 mencionadas anteriormente para el primer modo de realización.

Un programa informático que incluya unas instrucciones para la implementación del procedimiento según la invención puede realizarse por expertos en la materia según un algoritmo general deducido de los diagramas de las figuras 2 a 4, y de la presente descripción detallada.

La figura 5 ilustra esquemáticamente la estructura de los elementos comprendidos en un sistema de la figura 1. Cada dispositivo (el terminal, la entidad de gestión de servicio o la entidad de acceso) incluye una unidad de procesamiento 50 configurada para implementar las etapas correspondientes del procedimiento, por ejemplo implementando un programa informático según un modo de realización de la invención. Cada dispositivo incluye además una unidad de memoria 51 para almacenar unos datos de cálculo o para almacenamiento de un programa informático según la presente invención para su ejecución por un procesador de la unidad de procesamiento. Cada dispositivo incluye además una unidad de comunicación 52 para comunicar principalmente con los otros dispositivos del sistema o con las bases de datos 12 y 15 según la invención.

La presente invención no se limita a las formas de realización presentadas. Pueden deducirse e implementarse por un experto en la materia otras variantes y modificaciones de realización con la lectura de la presente descripción y de las figuras adjuntas.

REIVINDICACIONES

1. Procedimiento de acceso a un flujo de datos de contenido por un terminal de telecomunicaciones (10), siendo transmitido dicho flujo a través de una red de comunicación (14) a la que está conectada una entidad de acceso (13) encargada de la distribución final del flujo, que incluye las etapas siguientes, implementadas por el terminal:

- envío (S200) de una primera solicitud (Solic1) con destino a una entidad de gestión de acceso a un servicio (11), dirigiéndose esta primera solicitud a identificar el terminal ante la entidad de gestión de acceso al servicio (11),
- después de la identificación del terminal por la entidad de gestión de acceso al servicio (11), recepción (S202, S303) de medios de autenticación (K1, Cert) proporcionados por la entidad de gestión de acceso al servicio (11),
- envío (S204, S304, S405) de una segunda solicitud (Solic2) con destino a una entidad de acceso (13), dirigiéndose esta segunda solicitud al acceso por el terminal al flujo de datos de contenido, y siendo generada esta segunda solicitud utilizando los medios de autenticación proporcionados por la entidad de gestión de acceso al servicio (11), y
- recepción procedente de la entidad acceso (13) de un flujo de datos de contenido, tras una autenticación positiva del terminal ante la entidad de acceso (13).

2. Procedimiento según la reivindicación 1, que incluye además una etapa de determinación (S201) de uno o varios derechos de acceso del terminal a uno o varios flujos de datos por la entidad de gestión de acceso al servicio.

3. Procedimiento según la reivindicación 1, en el que la primera solicitud y/o la segunda solicitud incluye al menos uno de entre un identificador del terminal y de una dirección de red del terminal

4. Procedimiento según la reivindicación 1, en el que los medios de autenticación incluyen una primera clave criptográfica para firmar la segunda solicitud.

5. Procedimiento según la reivindicación 4, en el que la entidad de acceso autentica la segunda solicitud verificando la firma de la segunda solicitud por medio de la primera clave criptográfica.

6. Procedimiento según una de las reivindicaciones 4 y 5, en el que la primera clave criptográfica se obtiene dinámicamente a partir de al menos uno de entre un identificador del terminal y una dirección de red del terminal.

7. Procedimiento según la reivindicación 1, en el que los medios de autenticación incluyen un certificado de autenticación que autoriza el acceso por el terminal al flujo de datos.

8. Procedimiento según la reivindicación 7, en el que el certificado incluye además una duración de validez del certificado.

9. Procedimiento según la reivindicación 7 u 8, en el que el certificado incluye al menos uno de entre un identificador de línea telefónica y un número de puerto en el que está conectada la línea telefónica a la entidad de acceso.

10. Procedimiento según una de las reivindicaciones 7 a 9, en el que la segunda solicitud incluye el certificado.

11. Procedimiento según una de las reivindicaciones 7 a 10, en el que la entidad de acceso verifica el certificado por medio de una segunda clave de autoridad de certificación.

12. Procedimiento según una de las reivindicaciones 7 a 11, en el que la segunda solicitud está firmada por el terminal por medio de una tercera clave criptográfica.

13. Procedimiento según la reivindicación 12, en el que la entidad de acceso autentica la segunda solicitud verificando la firma de la segunda solicitud por medio de la tercera clave criptográfica.

14. Programa informático que incluye unas instrucciones para la implementación de un procedimiento según una de las reivindicaciones precedentes, cuando el programa lo ejecuta un procesador.

15. Terminal de telecomunicaciones (10) configurado para acceder a un flujo de datos de contenido, siendo transmitido dicho flujo a través de una red de telecomunicaciones (14) a la que se conecta una entidad de acceso (13), encargada de la distribución final del flujo, que incluye:

- una unidad de comunicación (42) configurada para enviar una primera solicitud (Solic1) con destino a una entidad de gestión de acceso a un servicio (11), dirigiéndose esta primera solicitud a identificar el terminal ante la entidad de gestión de acceso a un servicio (11), para recibir unos medios de autenticación (K1, Cert) proporcionados por la entidad de gestión de acceso al servicio (11) después de la identificación del terminal por la entidad de gestión de acceso al servicio (11), para enviar una segunda solicitud (Solic2) con destino a una entidad de acceso (13), dirigiéndose esta segunda solicitud al acceso por el terminal al flujo de datos de

contenido, y para recibir, procedente de la entidad de acceso (13), un flujo de datos de contenido, tras una autenticación positiva del terminal ante la entidad de acceso (13), y

- una unidad de tratamiento (40) configurada para generar la segunda solicitud utilizando los medios de autenticación proporcionados por la entidad de gestión de acceso al servicio (11).

16. Sistema de distribución de flujos de datos de contenidos a través de una red de telecomunicaciones (14), que incluye:

- un terminal (10) de telecomunicaciones según la reivindicación 15,
- una entidad de gestión de acceso a un servicio (11), configurada para recibir una primera solicitud (Solic1) enviada por el terminal, dirigiéndose esta primera solicitud a identificar el terminal ante la entidad de gestión de acceso al servicio (11), para enviar unos medios de autenticación (K1, Cert) después de la identificación del terminal, y
- una entidad de acceso (13) encargada de la distribución final del flujo al terminal, configurada para recibir una segunda solicitud (Solic2) enviada por el terminal, dirigiéndose la segunda solicitud al acceso por el terminal al flujo de datos de contenido, para autenticar al terminal en función de la segunda solicitud, generada por el terminal utilizando dichos medios de autenticación, y para transmitir el flujo de datos requerido una vez autenticado el terminal.

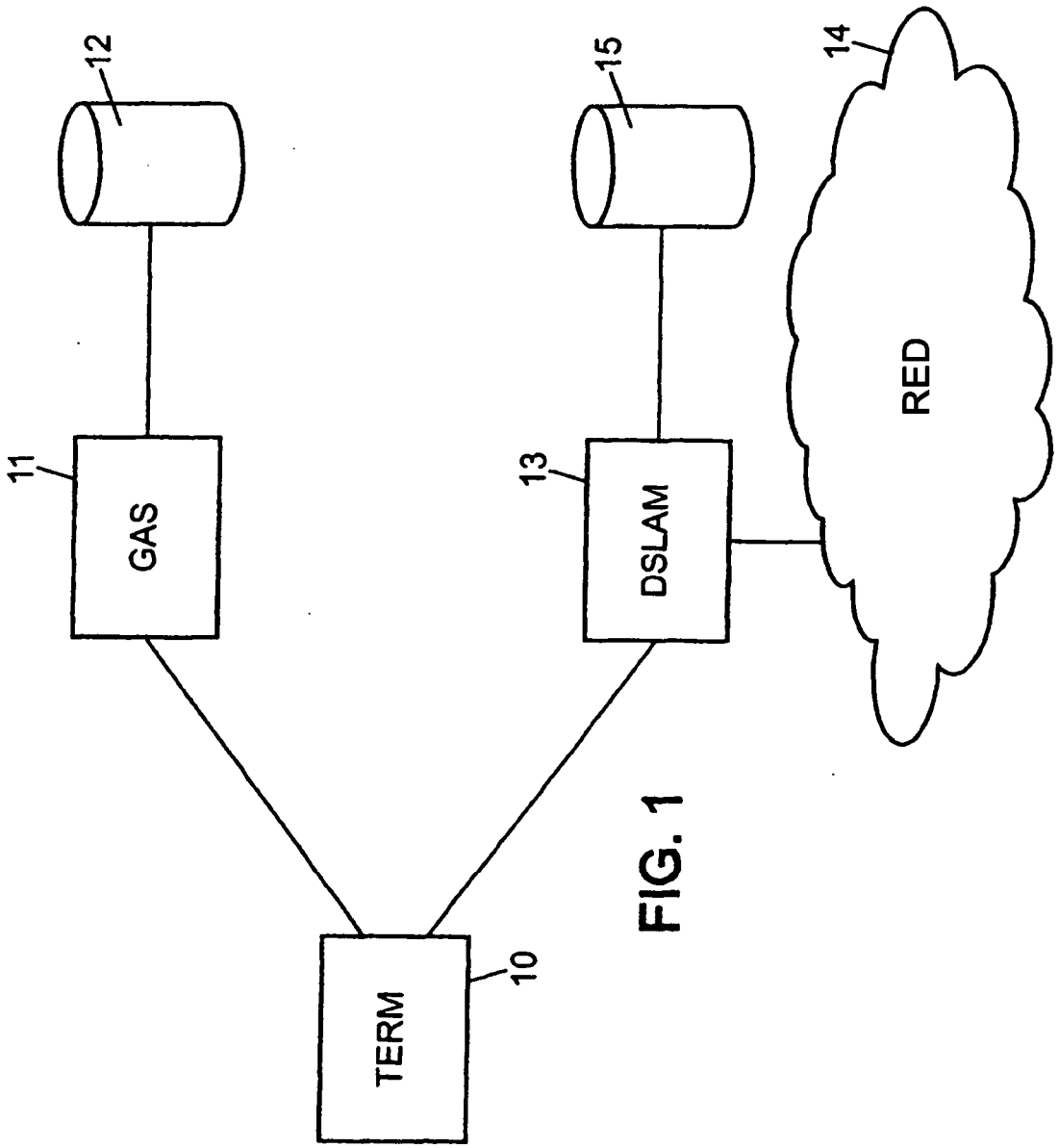


FIG. 1

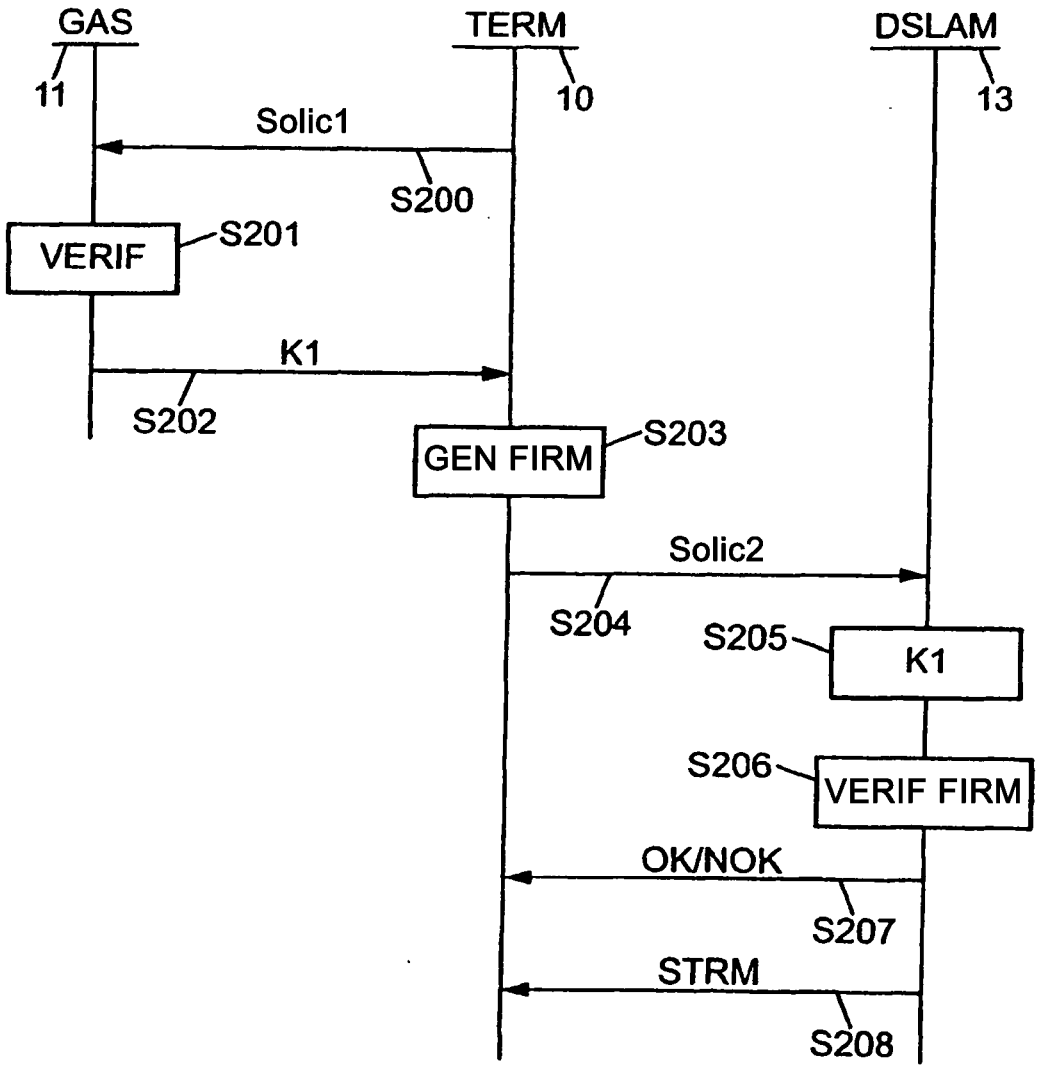

GAS
TERM
DSLAM
11
10
13
Solic1
S200
VERIF
S201
K1
S202
GEN FIRM
S203
Solic2
S204
S205
K1
S206
VERIF FIRM
OK/NOK
S207
STRM
S208

FIG. 2

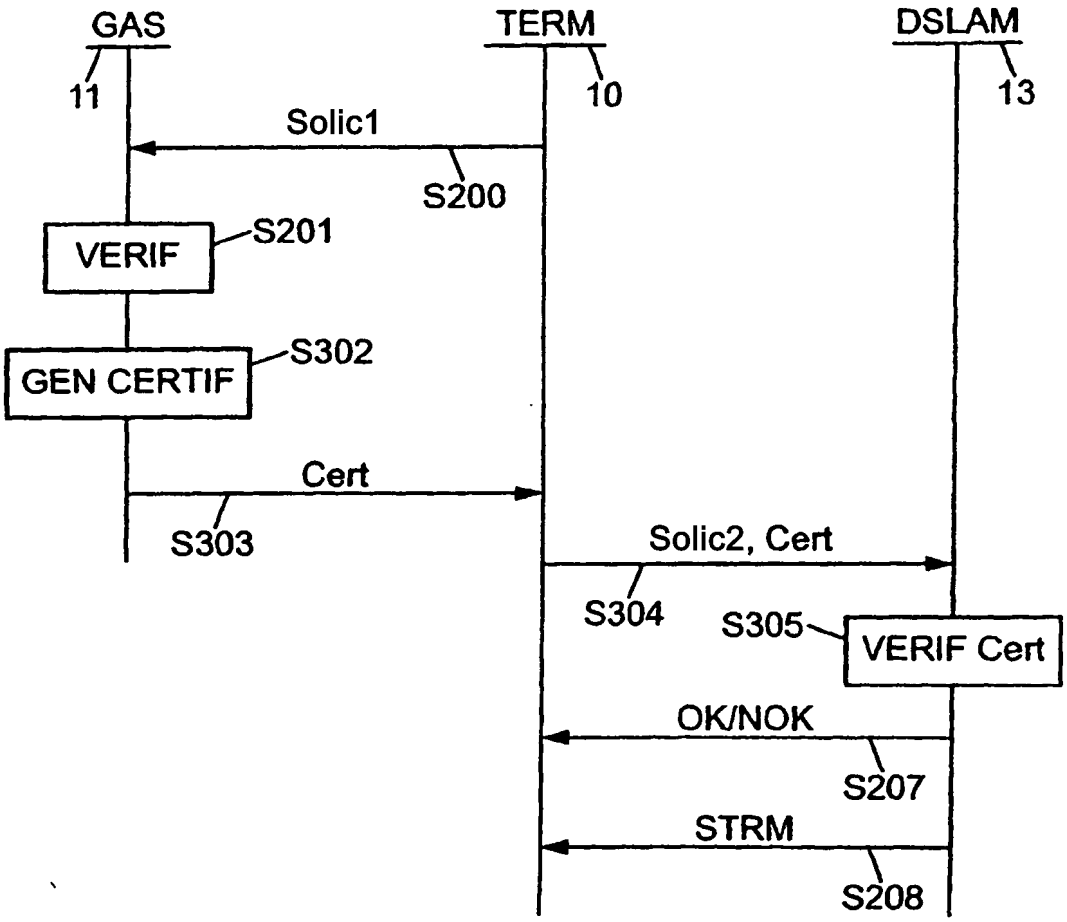

GAS
TERM
DSLAM
11
10
13
Solic1
S200
VERIF
S201
GEN CERTIF
S302
Cert
S303
Solic2, Cert
S304
S305
VERIF Cert
OK/NOK
S207
STRM
S208

FIG. 3

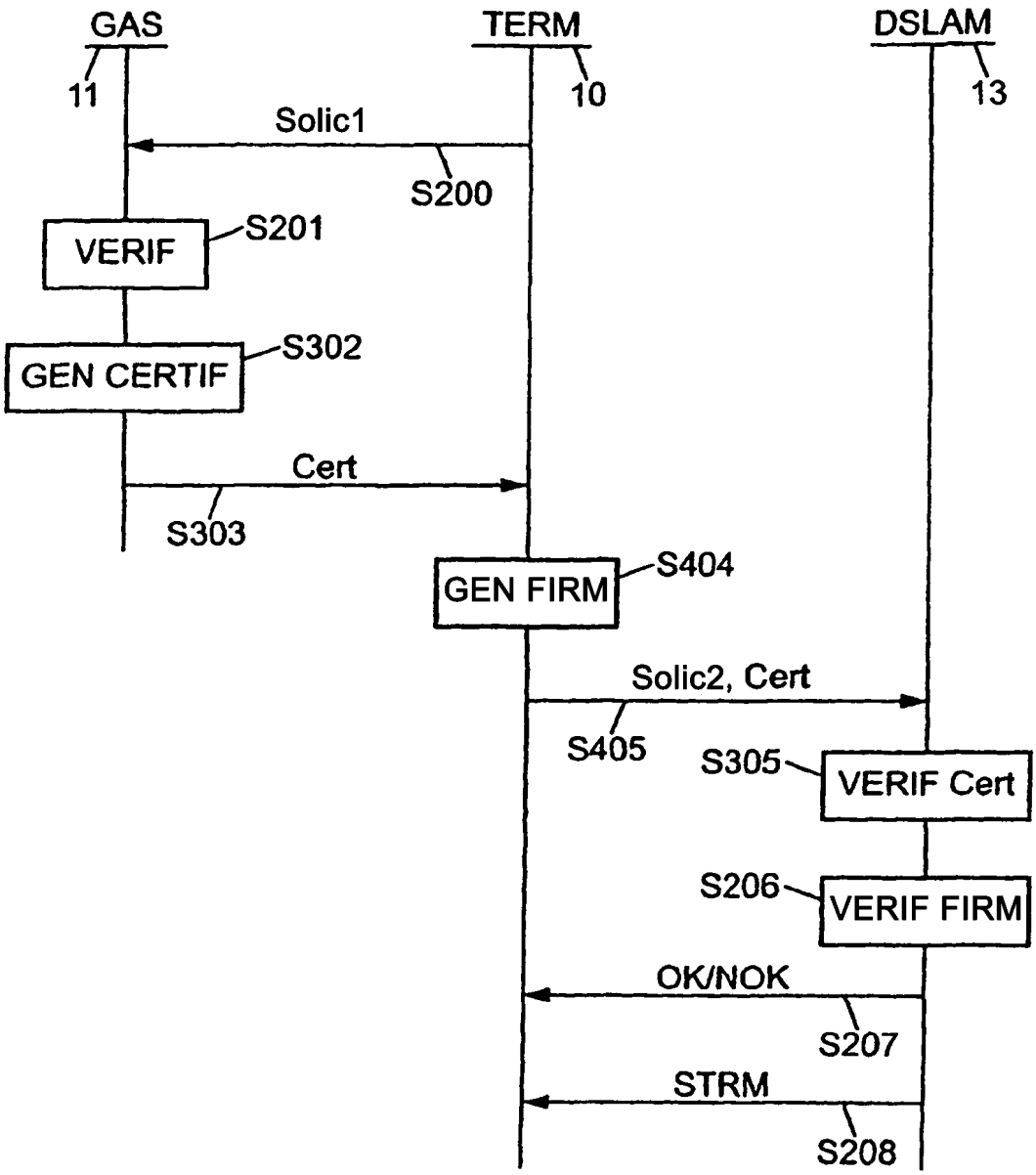
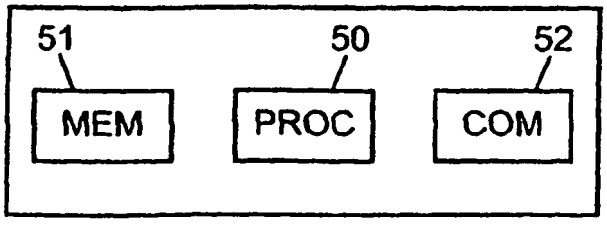

GAS
TERM
DSLAM
11
10
13
Solic1
S200
VERIF
S201
GEN CERTIF
S302
Cert
S303
GEN FIRM
S404
Solic2, Cert
S405
S305
VERIF Cert
S206
VERIF FIRM
OK/NOK
S207
STRM
S208

FIG. 4

FIG. 5


51
50
52
MEM
PROC
COM