(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 406 946**

(51) Int. CI.:

H04L 29/12 (2006.01)
H04L 29/06 (2006.01)
G06F 17/30 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.10.2006 E 06831295 (8)**

(97) Fecha y número de publicación de la concesión europea: **13.02.2013 EP 1941705**

(54) Título: **Procedimiento y sistema de protección de un enlace de acceso a un servidor**

(30) Prioridad:

26.10.2005 FR 0510921

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.06.2013

(73) Titular/es:

FRANCE TELECOM (100.0%)
78 rue Olivier de Serres
75015 PARIS, FR

(72) Inventor/es:

LOTTIN, PHILIPPE;
LE MERCIER, CLAUDINE y
REY, JEAN-FRANÇOIS

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Procedimiento y sistema de protección de un enlace de acceso a un servidor

Campo de la invención

La invención se refiere al aseguramiento del acceso a datos almacenados en un servidor remoto, siendo accesibles los datos por la difusión de un enlace de acceso (por ejemplo dirección URL, email IP, etc.). Se refiere particularmente al aseguramiento del acceso a un medio o una información relativa a un llamador frente a un llamado.

Técnica anterior

Una dirección electrónica, como por ejemplo de tipo URL (*Uniform Resource Locator*), es un formato de nombres de dominio universal que permite designar el emplazamiento de un recurso (datos, imágenes, videos, sonidos, etc.) en la red Internet. En ciertos casos, es importante proteger el acceso directo a los recursos.

En el caso por ejemplo de un servicio de presentación de identidad OIP (*Originating Identification Presentation*) durante una comunicación (voz, datos) como por ejemplo una llamada telefónica del tipo voz sobre IP (*Internet Protocol*), el interlocutor solicitado puede recibir una tarjeta de identidad multimedia del llamador. A tal fin, un enlace correspondiente a una dirección electrónica (por ejemplo dirección URL) es recibido por el llamado para permitirle acceder a la tarjeta de identidad multimedia del llamador registrado en la agenda de red del llamador que es accesible por mediación de este enlace en un servidor remoto. En ausencia de aseguramiento, el conocimiento de esta dirección puede permitir al llamado consultar toda la agenda del llamador (informaciones personales y contactos del llamador), incluso modificar o falsificar los datos de la agenda.

Para limitar los ataques directos del exterior, se puede utilizar un servidor llamado servidor “proxy invertido” que permite enmascarar la conexión al servidor de contenido que contiene realmente los recursos. Se interpone como repetidor entre el cliente y el servidor de contenido volviendo a este último invisible para el cliente. El servidor proxy invertido traduce una dirección URL de la red pública que la recibe en una dirección URL privada y transfiere el contenido al cliente como si respondiese él mismo a la petición de solicitud de contenido enviado por el cliente.

El documento *Running a Reverse Proxy with Apache* de Nick Kew, disponible en la URL http://www.apacheweek.com/features/reverseproxies, da un ejemplo de servidor proxy invertido.

No obstante, igual con esta solución, el llamado o un tercero dispone de un acceso permanente a los datos de la agenda del llamador que pueden entonces al menos ser copiados y utilizados por otros servicios.

Objeto y descripción sucinta de la invención

La presente invención tiene por objeto remediar los inconvenientes precitados y proponer una solución para poner a disposición de forma asegurada contenidos multimedia, y esto para una duración limitada definida ya sea por anticipado, ya sea en función de acontecimientos predeterminados.

Este objeto se alcanza gracias a un procedimiento de aseguramiento del acceso a datos almacenados en un servidor de contenido remoto, siendo accesibles dichos datos desde un terminal por medio de una dirección electrónica (URL, dirección email, número de teléfono, dirección IP, etc.), caracterizado porque comprende las siguientes etapas:

a) una etapa de creación, para una duración de validez determinada, de una dirección electrónica de enmascaramiento, estando asociada dicha dirección electrónica de enmascaramiento a la dirección electrónica del servidor remoto en un servidor proxy invertido, y

b) una etapa de comunicación de la dirección electrónica de enmascaramiento por el servidor proxy invertido al terminal.

Así, el procedimiento de la invención permite asegurar la difusión de una dirección electrónica (URL, dirección mail, número de teléfono, dirección IP, etc.) que da acceso a recursos multimedia (imagen, video, sonido, etc.) o a informaciones personales que se desean presentar durante un tiempo limitado. En efecto, la asociación dirección electrónica de enmascaramiento / dirección electrónica del servidor de contenido que permite enmascarar la dirección electrónica real del servidor de contenido al cliente final no es operativa más que para una duración limitada. Se controla así la duración de puesta a disposición del contenido.

La duración de acceso a los datos del servidor de contenido puede ser definida en función de acontecimientos externos. En este caso, la etapa a) puede ser iniciada particularmente por la solicitud de establecimiento de una sesión de comunicación (por ejemplo emisión de una llamada de voz sobre IP de tipo llamada SIP) con destino al

terminal del llamado, comprendiendo el procedimiento además una etapa c) de desactivación de la dirección electrónica de enmascaramiento en el servidor proxy invertido que puede ser iniciada ya sea después de una duración predeterminada (por ejemplo desactivación de la dirección electrónica de enmascaramiento al cabo de dos segundos después de la aceptación de la sesión de comunicación por el llamado), ya sea a continuación de un acontecimiento en la red de comunicación como por ejemplo en el momento de la aceptación de la sesión de comunicación (por ejemplo llamada SIP) por el llamado o al final de la sesión de comunicación.

Eso permite, en la etapa a), que un servidor de aplicación OIP reaccione a la solicitud de establecimiento de la sesión de comunicación (por ejemplo emisión de una llamada SIP) por un llamador con destino al terminal del llamado consultando una base de datos en conexión con el servidor de contenido para determinar la dirección electrónica de los datos de identidad del llamador para transmitir al terminal del llamado y asociando a esta dirección electrónica la dirección electrónica de enmascaramiento, siendo transmitidas las dos direcciones electrónicas asociadas al servidor proxy invertido.

En este caso, el procedimiento de la invención permite responder a la cuestión de confidencialidad de las informaciones personales del llamador disponibles para el llamado a partir de la agenda de contactos del llamador (fotos, datos de contactos, etc.), evitar la copia de contenido entre diferentes servicios y proteger la agenda de contactos del llamador de un acceso directo por el llamado o un tercero.

Según un aspecto de la invención, el procedimiento comprende además una etapa de consulta por el servidor de aplicación OIP de la base de datos para verificar si el usuario destinatario de la sesión de comunicación está autorizado a acceder a los datos de identidad del llamador. El llamador puede configurar su agenda de contactos prohibiendo a ciertos contactos tener acceso a su agenda para la presentación de identidad personalizada (por ejemplo tarjeta de identidad multimedia). El usuario tiene así la posibilidad de incrementar además el nivel de seguridad prohibiendo el acceso de a agenda a algunos de sus contactos.

La presente invención se refiere igualmente a un sistema de aseguramiento del acceso a datos almacenados en un servidor de contenido remoto, siendo accesibles dichos datos desde un terminal por medio de una dirección electrónica, caracterizado porque comprende además un servidor de aplicación para crear, para una duración de validez determinada, una dirección electrónica de enmascaramiento y para transmitir dicha dirección electrónica de enmascaramiento asociada a la dirección electrónica del servidor remoto a un servidor proxy invertido, accediendo el terminal temporalmente a los datos almacenados en el servidor de contenido por medio de la dirección electrónica de enmascaramiento por mediación del servidor proxy invertido.

Igual que para el procedimiento descrito anteriormente, el sistema de la invención comprende unos medios (servidor de aplicación) para crear una asociación entre la dirección electrónica real del servidor de contenido y una dirección electrónica de enmascaramiento y transmitir esta asociación a un servidor proxy invertido que vuelve invisible la dirección electrónica del servidor de contenido para el cliente. El servidor de aplicación controla además la duración de validez de esta asociación para limitar a una duración determinada el acceso por el terminal del cliente a los datos almacenados en el servidor de contenido.

El sistema de la invención puede ser puesto en marcha en una red de comunicaciones de tipo NGN (*Next Generation Network*) que utiliza las tecnologías de transporte en modo paquete. En este caso, el servidor de aplicación es un servidor de aplicación OIP y comprende unos medios que reaccionan a la emisión de una solicitud de sesión de comunicación (por ejemplo llamada SIP) por un llamador con destino al terminal de un llamado consultando una base de datos en conexión con el servidor de contenido para determinar la dirección electrónica de los datos de identidad del llamador para transmitir al terminal y asociando a esta dirección electrónica la dirección electrónica de enmascaramiento, siendo transmitidas las dos direcciones electrónicas asociadas al servidor proxy invertido.

El servidor de aplicación OIP comprende además unos medios para desactivar la asociación entre la dirección electrónica de enmascaramiento y la dirección electrónica del servidor remoto en el servidor proxy invertido ya sea después de una duración predeterminada (por ejemplo desactivación de la dirección electrónica de enmascaramiento al cabo de dos segundos después de la aceptación de la sesión de comunicación por el llamado), ya sea a continuación de un acontecimiento en la red de comunicación como por ejemplo en el momento de la aceptación de la sesión de comunicación por el llamado o al final de esta sesión.

El acceso a la agenda del llamador para permitir la presentación de las informaciones de identidad del llamador no es accesible para el llamado más que durante una duración limitada y por mediación de una dirección electrónica de enmascaramiento.

El servidor de aplicación OIP puede comprender además unos medios para verificar si el usuario destinatario de la sesión de comunicación está autorizado a acceder a los datos de identidad del llamador. Esto permite al llamado prohibir el acceso a su agenda a algunos de sus contactos.

La invención se refiere además a un servidor de aplicación en conexión con una red de transmisión de datos en el que datos almacenados en un servidor de contenido remoto son accesibles desde un terminal por medio de una

dirección electrónica, caracterizado porque comprende unos medios para crear temporalmente una dirección electrónica de enmascaramiento asociada a una dirección electrónica del servidor de contenido remoto y para transmitir las dos direcciones asociadas a un servidor proxy invertido en conexión con el terminal.

En el caso de una red de telecomunicación en modo paquete con servicio de presentación de identidad OIP, el servidor de aplicación comprende además unos medios que reaccionan a la emisión de una solicitud de sesión de comunicación por un llamador con destino a dicho terminal consultando una base de datos en conexión con el servidor de contenido para determinar la dirección electrónica de los datos de identidad del llamador para transmitir al terminal y asociando a esta dirección electrónica la dirección electrónica de enmascaramiento, siendo transmitidas las dos direcciones electrónicas asociadas al servidor proxy invertido. Comprende además unos medios que reaccionan ya sea a un acontecimiento temporal (por ejemplo desactivación de la dirección electrónica de enmascaramiento al cabo de dos segundos después de la aceptación de la sesión de comunicación por el llamado), ya sea en un acontecimiento en la red de comunicación (aceptación de la sesión de comunicación por el llamado o fin de la sesión) desactivando la asociación entre la dirección electrónica de enmascaramiento y la dirección electrónica del servidor remoto en el servidor proxy invertido.

La invención se refiere finalmente a un programa de ordenador destinado a ser puesto en marcha en un servidor de aplicación tal como el descrito precedentemente, caracterizado porque comprende instrucciones para crear temporalmente una dirección electrónica de enmascaramiento asociada a una dirección electrónica de un servidor de contenido remoto y para transmitir las dos direcciones asociadas a un servidor proxy invertido en conexión con el terminal.

El programa puede comprender además instrucciones para reaccionar a la emisión de una solicitud de sesión de comunicación por un llamador consultando una base de datos en conexión con el servidor de contenido para determinar la dirección electrónica de los datos de identidad del llamador para transmitir y asociando a esta dirección electrónica la dirección electrónica de enmascaramiento, e instrucciones para reaccionar ya sea a un acontecimiento temporal (por ejemplo desactivación de la dirección electrónica de enmascaramiento al cabo de dos segundos después de la aceptación de la sesión de comunicación por el llamado), ya sea a un acontecimiento en la red de comunicación (aceptación de la sesión de comunicación por el llamado o fin de la sesión) desactivando la asociación entre la dirección electrónica de enmascaramiento y la dirección electrónica del servidor remoto en el servidor proxy invertido.

Breve descripción de los dibujos

Otras características y ventajas de la invención surgirán de la descripción siguiente de modos particulares de realización de la invención, dados a modo de ejemplos no limitativos, en referencia a los dibujos adjuntos, en los que:

- la figura 1 es una vista esquemática global de un modo de realización de un sistema de protección de un enlace de acceso a un servidor según la invención,

- la figura 2 muestra un primer ejemplo de puesta en marcha en un sistema de protección de un enlace de acceso a un servidor según la invención,

- la figura 3 muestra un segundo ejemplo de puesta en marcha en un sistema de protección de un enlace de acceso a un servidor según la invención,

- la figura 4 muestra un tercer ejemplo de puesta en marcha en un sistema de protección de un enlace de acceso a un servidor según la invención.

Descripción detallada de modos de realización de la invención

La presente invención propone una solución para permitir la protección del acceso a datos almacenados en un servidor y accesibles por mediación de una dirección electrónica que puede ser de cualquier tipo y particularmente de tipo URL (*Uniform Ressource Locator*), dirección email, dirección IP (*Internet Protocol*), número de teléfono, etc. Los datos pueden ser de cualquier tipo (imágenes, sonidos, video, etc.). De una manera general, el principio de protección de la invención asocia la utilización de un servidor proxy invertido para enmascarar la dirección electrónica real del servidor que da acceso a los datos con un servidor de aplicación que controla el servidor proxy invertido para crear en este último una dirección electrónica de enmascaramiento con una duración de validez limitada en el tiempo. Así, como se explica más adelante en detalle, el usuario destinado a acceder a los datos no podrá hacerlo más que a partir de una dirección electrónica de enmascaramiento (es decir, ignorando la dirección electrónica real) y solamente para una duración limitada.

De forma no limitativa, la presente invención se aplica ventajosamente a la tecnología reciente de las sesiones de comunicación de voz y/o datos como por ejemplo las llamadas telefónicas voz sobre IP de tipo llamadas SIP (*Session Initiation Protocol*), siendo SIP un protocolo conocido que permite crear y gestionar sesiones entre usuarios

para establecer conversación telefónicas de tipo voz sobre IP (o VoIP, *Voice on Internet Protocol*), es decir utilizando protocolos de transporte (transmisión por paquetes) que hasta aquí estaban reservados al transporte de datos). A modo de ejemplo, las sesiones de comunicaciones establecidas entre un llamador/solicitante A y un llamado/solicitado B pueden ser puestas en marcha siguiendo el protocolo conocido H323 (protocolo definido por la ITU (*International Telecommunications Union*) que permite la puesta en relación IP (sesión) entre dos puntos en una red de comunicación).

La figura 1 ilustra una arquitectura de un sistema de comunicación con presentación de datos de identificación de llamador en la que la presente invención puede ser puesta en marcha. En interés de la simplificación pero de manera no limitativa, en los ejemplos descritos a continuación la dirección electrónica corresponderá a una dirección URL mientras que la sesión de comunicación corresponderá a una llamada SIP.

La arquitectura de la figura 1 comprende dos terminales 1 y 2 capaces de conectarse a una red 3 de tipo red NGN (*Next Generation Network*, nueva arquitectura de red de comunicación cuyo principio es utilizar las tecnologías de transporte en modo paquete, reservadas hasta entonces para los datos, para transportar el conjunto de los servicios de telecomunicaciones). Este tipo de red permite particularmente la puesta en marcha del servicio OIP (*Originating Identification Presentation*) que permite la presentación de datos de identificación del llamador en el terminal del llamado durante una llamada. El servicio presentación de datos de identidad OIP es denominado CLIP (*Calling Line Identification Presentation*) en la red RTC (Red Telefónica Conmutada) y RNIS (Red Numérica con Integración de Servicios) y es normalizado en el ETSI bajo la especificación ETSI EN 300 089 *Integrated Services Digital Network* (ISDN); *Calling Line Identification Presentation* (CLIP) *supplementary service; Service description*. Concretamente, este servicio permite al llamado recibir en su terminal una tarjeta de identidad o tarjeta de visita multimedia del llamador durante la recepción de una llamada de este último.

Como se ha descrito en detalle en las solicitudes de patente FR 0510387 y FR 0510389, tal tarjeta de identidad puede comprender particularmente informaciones multimedia tales como un anuncio, un enlace hacia un sitio personal, un avatar, una foto, una banda sonora, etc. Estas tarjetas son creadas por el llamador y memorizadas con su lista de contactos igualmente llamada agenda NAB (*Network Address Book*). En efecto, el llamador asocia cada tarjeta de identidad que ha creado a varios contactos de su agenda NAB para que estos reciban automáticamente la tarjeta correspondiente durante una llamada. La puesta en marcha del envío de estas tarjetas simultáneamente en la llamada telefónica es igualmente descrita en detalle en las solicitudes de patente citadas precedentemente.

El sistema de la figura 1 comprende además un servidor 5 de aplicación OIP en el que es implementado el servicio OIP, un servidor proxy dinámico invertido 6 y una base de datos de contactos 4 accesible por un servidor 41.

En interés de la simplificación, en el resto de la descripción se considera que los terminales 1 y 2 pertenecen respectivamente a un llamador A y un llamado B. Se considera además que el servicio OIP es activado al menos en la línea del llamado B.

Conforme a la invención, el servidor 5 de aplicación OIP gestiona el servicio de presentación de identidad OIP. Tras la recepción de una llamada (solicitud de establecimiento de una sesión de comunicación), el servidor 5 de aplicación OIP consulta la base de datos de contactos 4 por mediación del servidor 41 para conocer la dirección URL real de las informaciones que debe transmitir al llamado B. Crea después una dirección URL de enmascaramiento y transmite estas dos informaciones al proxy dinámico invertido 6 durante la activación. Esta dirección URL de enmascaramiento es insertada en la llamada enviada al llamado B.

Después de una duración predeterminada (por ejemplo desactivación de la dirección URL de enmascaramiento al cabo de dos segundos después de la aceptación de la llamada SIP por el llamador) o a continuación de un acontecimiento en la red como por ejemplo en el momento de la aceptación de la llamada SIP por el llamado o al final de la llamada SIP cuando el llamado cuelga, el servidor de aplicación OIP desactiva esta asociación en el lado del proxy dinámico invertido.

El servidor proxy dinámico invertido 6 gestiona, en un servicio de presentación de identidad OIP de A a B, la asociación entre las direcciones URL reales hacia los servidores de contenido (aquí el servidor o servidores 41 que alojan la base de datos de contactos 4) y las direcciones URL de enmascaramiento creadas por el servidor 5 de aplicación OIP.

Tras la recepción de una llamada (mensajes M1 y M2 en la figura 1) el servidor 5 de aplicación OIP activa una nueva asociación. Tras la recepción de una petición del llamado B (mensaje M7) en la dirección URL de enmascaramiento, el servidor proxy dinámico invertido 6 consulta la dirección URL real (mensaje M8) y después retransmite el contenido al llamado B enmascarando totalmente el servidor que alberga la dirección URL real (mensaje 9).

Después de una duración predeterminada o a continuación de un acontecimiento en la red (por ejemplo principio o fin de la sesión de comunicación), el servidor 5 de aplicación OIP desactiva la asociación precedente volviendo inaccesible la dirección URL real por mediación de la dirección URL de enmascaramiento. Los datos de identidades del llamador, como su tarjeta de identidad multimedia, transmitidos durante la duración de la activación de la

dirección URL de enmascaramiento en el servidor proxy dinámico invertido 6, pueden ser conservados temporalmente en memoria en el terminal 4 del llamado B con el fin de permanecer fijos en el terminal después de la desactivación de la dirección URL de enmascaramiento. La duración de activación de la dirección URL de enmascaramiento y, por consiguiente, el acceso indirecto al servidor de contenido puede ser reducido al mínimo necesario en la transmisión de las informaciones en el terminal del llamado, conservando este último después estos datos en la pantalla.

Más allá de su duración de activación, la dirección URL de enmascaramiento y, por supuesto, la dirección URL real son inaccesibles a los usuarios de la red.

Se puede, por ejemplo, utilizar el servidor HTTP Apache que permite poner en marcha un servidor proxy invertido HTTP por configuración. Permite así enmascarar direcciones URL privadas relevando mediante su intermediación el contenido resultante de estas direcciones hacia los terminales remotos llamadores de las peticiones de contenido.

No obstante, en el marco de la invención, este servidor no permite activar y desactivar la asociación dirección URL pública / dirección URL privada (aquí dirección URL real / dirección URL de enmascaramiento) en función de un acontecimiento exterior, particularmente una llamada SIP. La asociación es permanente, y no es dinámica. Para poner en marcha el servidor proxy dinámico invertido de la invención, hace falta además un control de la activación/desactivación de la asociación dirección URL real / dirección URL de enmascaramiento realizada por el servidor 5 de aplicación OIP tal como el descrito precedentemente.

La base de datos de contactos 4 contiene la lista de los contactos igualmente llamada agenda NAB (*Network Address Book*). Los datos almacenados en esta base (por ejemplo tarjetas de identidad multimedia) son accesibles por mediación de una dirección URL (dirección URL “real”).

La base 4 de datos que contiene la lista de los contactos del llamador A se encarga del intercambio interactivo con el llamador particularmente para crear las tarjetas de identidad multimedia y para parametrizar eventualmente el servicio de restricción de identidad para uno o varios contactos de la lista (transmisión Msyinc en la figura 1). Este intercambio utiliza las técnicas habituales de tipo:

- servidor vocal interactivo (aplicación VoiceXML, o arborescencia audiovisual, o cualquier otra técnica que permite un diálogo automatizado): recibe las órdenes del usuario en forma de frecuencias vocales (DTMF *Dual Tone Multi-Frequency*), por el desarrollo de un reconocimiento de palabra o cualquier otro dato informático, y/o

- página web, y/o

- interfaz hombre máquina (servidor gráfico)

Esta base de datos puede situarse en el servidor de la agenda NAB que es una agenda de red (por ejemplo agenda “mis contactos”), en el servidor de perfil del cliente (por ejemplo HSS, HLR), en el servidor de la agenda de una empresa, etc. En todos los casos, la base de datos es accesible por mediación de una dirección URL real.

Los terminales 1 y 2 son terminales capaces de establecer una comunicación (voz y/o datos) por mediación de la red 3 de tipo NGN. Además, para recibir una tarjeta de identidad multimedia, el llamado B debe utilizar un terminal 2 que comprende unos medios para recibir y visualizar datos multimedia (por ejemplo ordenador PC, aparato telefónico IP (*Internet Protocol*) SIP, etc.). Si en su agenda NAB, A ha activado el servicio de restricción de identidad para B, la identidad de A no será presentada a B sea cual sea el terminal utilizado por B.

Se describe ahora un ejemplo de puesta en marcha de la presente invención siempre en conexión con la figura 1 y que ilustra el acceso temporal a la agenda NAB del llamador A por el llamado B para permitir la presentación de la identidad de A a B durante la emisión de una llamada SIP de A a B.

El llamador A emite una petición de llamada con destino a un llamado B (mensajes M1, protocolo SIP) hacia la red 3 (por ejemplo red NGN) que reacciona haciendo una llamada al servicio de presentación de datos OIP (mensajes M2, protocolo SIP) implementado en el servidor 5 de aplicación OIP.

El servidor 5 de aplicación OIP consulta la base de datos de contactos 4 para conocer la agenda de red (NAB) de A y determinar si el llamado B tiene derecho a acceder a la misma (mensajes M3, protocolo XCAP (XML *Configuration Access Protocol*)/HTTP (*HyperText Transfer Protocol*)).

El servidor 5 de aplicación OIP que tiene conocimiento de la dirección URL real de la base 4 en la que se encuentra la agenda NAB de A, asocia esta dirección URL a una dirección URL de enmascaramiento. Transmite después al servidor proxy dinámico invertido 6 esta asociación (mensajes M4, protocolo XML/HTTP).

El servidor 5 de aplicación OIP emite entonces un mensaje hacia la red 3 (mensajes M5, protocolo SIP) que contacta con el llamado B (mensajes M6, protocolo SIP). Estos dos mensajes (mensajes M4 y M5) contienen la dirección URL

de enmascaramiento que permite acceder al servidor proxy dinámico invertido 6, y a continuación a la información de A en la NAB para esta llamada.

El llamado B contacta el servidor proxy dinámico invertido 4 por mediación de esta URL de enmascaramiento (mensajes M7, protocolo HTTP).

Con ayuda de la dirección URL real de la agenda NAB que conoce el servidor proxy dinámico invertido, consulta la agenda NAB de A (mensajes M8, protocolo HTTP). Devuelve después las informaciones de identidad contenidas en la agenda NAB de A al llamado B (mensajes M9, protocolo HTTP) que son notificadas a B por intermediación de los medios de visualización de su terminal 2.

La figura 2 muestra las etapas puestas en marcha en el sistema de la figura 1 (etapas que corresponden a intercambios de mensajes en un flujo multimedia Fm entre los diferentes elementos del sistema) durante una llamada SIP de A hacia B, teniendo B el derecho de conectarse a la agenda NAB de A durante la duración de la llamada conforme a la invención.

Como se describe precedentemente, cuando A emite una llamada con destino a B (etapa S1), el servidor 5 de aplicación OIP envía, por mediación de la dirección URL real de la base de datos de los contenidos 4, una solicitud para saber si B está autorizado a acceder a las informaciones de identidad de la agenda NAB de A (etapa S2). La base de datos de contactos 4 reenvía una respuesta que indica que B está autorizado a acceder a la agenda NAB de A (etapa S3). Cuando se recibe la respuesta, el servidor de aplicación OIP crea, para la duración de la llamada, la asociación “dirección URL de enmascaramiento creada / dirección URL real de la agenda NAB” que envía al servidor proxy dinámico invertido 6 (etapa S4). Después del acuse de recibo de esta asociación por el servidor 6 (etapa S5), la llamada de A es transmitida a B con la dirección URL de enmascaramiento que permite al terminal 2 de B acceder, para esta llamada, a las informaciones de identidades de A contenidas en su agenda NAB (etapa S6). Para obtener estas informaciones, el terminal 2 de B envía al servidor proxy dinámico invertido 6 una petición con la dirección de enmascaramiento (etapa S7). El servidor proxy dinámico invertido redirige la petición hacia la base de datos de contactos 4 utilizando su dirección URL real (etapa 8). La base 4 devuelve en respuesta las informaciones de identidad (por ejemplo tarjeta de identidad multimedia) de A disponibles en la agenda NAB (etapa S9) al servidor proxy dinámico invertido 6 que las redirige hacia el terminal 2 de B (etapa 10).

Cuando B cuelga (etapa S11), el servidor 5 de aplicación OIP entra en conexión con el servidor proxy dinámico invertido 6 para desactivar la asociación “dirección URL de enmascaramiento creada / dirección URL real de la agenda NAB” poniendo así fin a la posibilidad del terminal 2 de B de acceder a las informaciones de la agenda NAB de A en la base 5 (etapa S12). El servidor 5 de aplicación OIP informa por último al terminal 1 de A que B ha colgado y que la llamada está terminada. Como se describe precedentemente, la desactivación de la asociación “dirección URL de enmascaramiento creada / dirección URL real de la agenda NAB” puede así ser iniciada después de una duración predeterminada (por ejemplo desactivación de la dirección URL de enmascaramiento al cabo de dos segundos después de la aceptación de la llamada SIP por el llamado) o a continuación de un acontecimiento en la red como por ejemplo en el momento de la aceptación de la llamada SIP por el llamado.

La figura 3 muestra las etapas puestas en marcha en el sistema de la figura 1 (etapas que corresponden a intercambios de mensajes en un flujo multimedia Fm entre los diferentes elementos del sistema) durante una llamada SIP de A hacia B, no teniendo B derecho a conectarse a la agenda NAB de A. En este ejemplo, A no ha activado el servicio de restricción de identidad OIR (*Originating Identification Restriction*), servicio que permite impedir la presentación de la identidad del llamador en un servicio OIP clásico. Este servicio es implementado por el servidor 5 de aplicación OIP en petición de A a partir de su terminal 1 (mensajes Msync en la figura 1). Este servicio se refiere a los datos de identidades básicas no multimedia y no personalizadas diferentes de las disponibles en la agenda NAB de A que han sido personalizadas por A para cada uno de los miembros de su lista de contactos.

Cuando A emite una llamada con destina a B (etapa S20), el servidor 5 de aplicación OIP envía, por mediación de la dirección URL real de la base de datos de contenidos 4, una solicitud para saber si B está autorizado a acceder a las informaciones de identidad de la agenda NAB de A (etapa S21). La base de datos de los contactos reenvía una respuesta que indica que B no está autorizado a acceder a la agenda NAB de A (etapa S22).

En este caso, la llamada de A es transmitida al terminal 2 de B pero sin ninguna dirección URL de enmascaramiento (etapa S23). El terminal 2 de B no puede acceder a las informaciones de identidades de A contenidas en su agenda NAB.

Más precisamente, el terminal 2 de B envía al servidor proxy dinámico invertido 6 una petición para tratar de obtener una dirección de enmascaramiento que le permita acceder a las informaciones de identidad personalizadas de A (etapa S24). El servidor proxy dinámico invertido 6 redirige la petición hacia la base de datos de contactos 4 (etapa S25). La base 4 devuelve una respuesta negativa “informaciones inexistentes o prohibidas” al servidor 6 (etapa S26) que la redirige hacia el terminal 2 de B (etapa S27).

Sin embargo, en el caso de un servicio de presentación de identidad OIP y ya que A no ha activado el servicio de restricción de identidad OIR, la identidad de A podrá igualmente ser presentada en B. Esta identidad no corresponde a los datos de identidad multimedia personalizados de A en su agenda NAB (por ejemplo tarjeta de identidad de A personalizado) sino a simples datos de identidad (es decir, apellido, número de llamada y dirección email de A no multimedia y no personalizados en función de B) suministrados por el servicio OIP normalizado por el ETSI (*European Telcommunications Standard Institute*).

La comunicación prosigue así hasta el final de la llamada SIP (etapa S28).

La figura 4 muestra las etapas puestas en marcha en el sistema de la figura 1 (etapas que corresponden a intercambios de mensajes en un flujo multimedia Fm entre los diferentes elementos del sistema) durante una llamada SIP de A hacia B, teniendo A activado el servicio de restricción de identidad OIR (*Originating Identification Restriction*), servicio que permite impedir la presentación de la identidad del llamador en un servicio OIP clásico.

Cuando A emite una llamada con destino a B (etapa S30), el servidor 5 de aplicación OIP envía, por mediación de la dirección URL real de la base de datos de contenidos 4, una solicitud para saber si B está autorizado a acceder a las informaciones de identidad de la agenda NAB de A (etapa S31). La base de datos de los contactos reenvía una respuesta que indica que A ha activado el servicio de restricción de identidad OIR (etapa S32).

En este caso, la llamada de A es transmitida al terminal 2 de B pero sin ninguna presentación de información de identidad de A (etapa S33).

La comunicación prosigue así hasta el fin de la llamada SIP (etapa S34).

Se constata que en el caso de que A active el servicio de restricción de identidad OIR, B no puede tener conocimiento de ninguna información que sea resultante de los datos de identidad básicos (es decir, apellido, número de llamada y dirección email de A no multimedia y no personalizados en función de B) suministrados por el servicio OIP normalizado por el ETSI o datos de identidad multimedia personalizados de A en su agenda NAB (por ejemplo tarjeta de identidad de A personalizada en función de B).

REIVINDICACIONES

1.- Procedimiento de aseguramiento del acceso a datos almacenados en un servidor (41) de contenido remoto, siendo accesibles dichos datos desde un terminal por medio de una dirección electrónica, comprendiendo el procedimiento las siguientes etapas:

- una etapa (S4) de creación de una dirección electrónica de enmascaramiento, estando asociada dicha dirección electrónica de enmascaramiento a la dirección electrónica del servidor remoto en un servidor proxy invertido (6), y

- una etapa (S6) de comunicación de la dirección electrónica de enmascaramiento por el servidor proxy invertido (6) al terminal (2),

caracterizado porque la dirección electrónica de enmascaramiento es creada para una duración de validez determinada.

2.- Procedimiento según la reivindicación 1, caracterizado porque la etapa a) (S4) es iniciada durante la emisión de una solicitud de establecimiento de una sesión de comunicación con destino a dicho terminal (2) y porque comprende además una etapa c) (S12) de desactivación de la dirección URL de enmascaramiento en el servidor proxy invertido (6) después de una duración predeterminada o en respuesta a un acontecimiento en la sesión de comunicación.

3.- Procedimiento según la reivindicación 2, caracterizado porque, en la etapa a) (S4), un servidor (5) de aplicación de presentación de identidad reacciona a la emisión de una solicitud de establecimiento de una sesión de comunicación por un llamador (A) con destino a dicho terminal (2) consultando una base (4) de datos en conexión con el servidor (41) de contenido para determinar la dirección electrónica de los datos de identidad del llamador (A) a transmitir al terminal y asociando a esta dirección electrónica la dirección electrónica de enmascaramiento, siendo transmitidas las dos direcciones electrónicas asociadas al servidor proxy invertido (6).

4.- Procedimiento según la reivindicación 3, caracterizado porque comprende además una etapa (S21) de consulta por el servidor (5) de aplicación de presentación de identidad de la base de datos (4) para verificar si el usuario (B) destinatario de la solicitud de establecimiento de una sesión de comunicación está autorizado a acceder a los datos de identidad del llamador (A).

5.- Sistema de aseguramiento del acceso a datos almacenados en un servidor (41) de contenido remoto, siendo accesibles dichos datos desde un terminal (2) por medio de una dirección electrónica, caracterizado porque comprende un servidor (5) de aplicación para crear una dirección electrónica de enmascaramiento y para transmitir dicha dirección electrónica de enmascaramiento asociada a la dirección electrónica del servidor remoto (41) a un servidor proxy invertido (6), siendo el terminal (2) capaz de acceder a los datos almacenados en el servidor (41) de contenido por medio de la dirección electrónica de enmascaramiento por mediación del servidor proxy invertido (6), caracterizado porque la dirección electrónica es creada para una duración determinada.

6.- Sistema según la reivindicación 5, caracterizado porque el servidor (5) de aplicación es un servidor de aplicación de presentación de identidad y porque comprende unos medios que reaccionan a la emisión de una solicitud de establecimiento de una sesión de comunicación por un llamador (A) con destino a dicho terminal (2) consultando una base (4) de datos en conexión con el servidor (41) de contenido para determinar la dirección electrónica de los datos de identidad del llamador (A) a transmitir al terminal (2) y asociando a esta dirección electrónica la dirección electrónica de enmascaramiento, siendo transmitidas las dos direcciones electrónicas asociadas al servidor proxy invertido (6).

7.- Sistema según la reivindicación 6, caracterizado porque el servidor (5) de aplicación de presentación de identidad comprende además unos medios para desactivar la asociación entre la dirección electrónica de enmascaramiento y la dirección electrónica del servidor remoto en el servidor proxy invertido (6) después de una duración predeterminada o en respuesta a un acontecimiento en la sesión de comunicación.

8.- Sistema según la reivindicación 6 ó 7, caracterizado porque el servidor (5) de aplicación de presentación de identidad comprende además unos medios para verificar si el usuario (B) destinatario de la solicitud de sesión de comunicación está autorizado a acceder a los datos de identidad del llamador (A).

9.- Servidor (5) de aplicación en conexión con una red de transmisión de datos en la que datos almacenados en un servidor (41) de contenido remoto son accesibles desde un terminal (2) por medio de una dirección electrónica, comprendiendo dicho servidor unos medios para crear una dirección electrónica de enmascaramiento asociada a una dirección electrónica del servidor (41) de contenido remoto y para transmitir las dos direcciones asociadas a un servidor proxy invertido (6) en conexión con el terminal (2), caracterizado porque la dirección electrónica de enmascaramiento es creada para una duración determinada.

10.- Programa de ordenador destinado a ser puesto en marcha en un servidor (5) de aplicación según la reivindicación 9, comprendiendo dicho programa instrucciones para crear una dirección electrónica de enmascaramiento asociada a una dirección electrónica de un servidor (41) de contenido remoto y para transmitir las dos direcciones asociadas a un servidor proxy invertido (6) en conexión con el terminal (2), caracterizado porque la dirección electrónica de enmascaramiento es creada para una duración determinada.

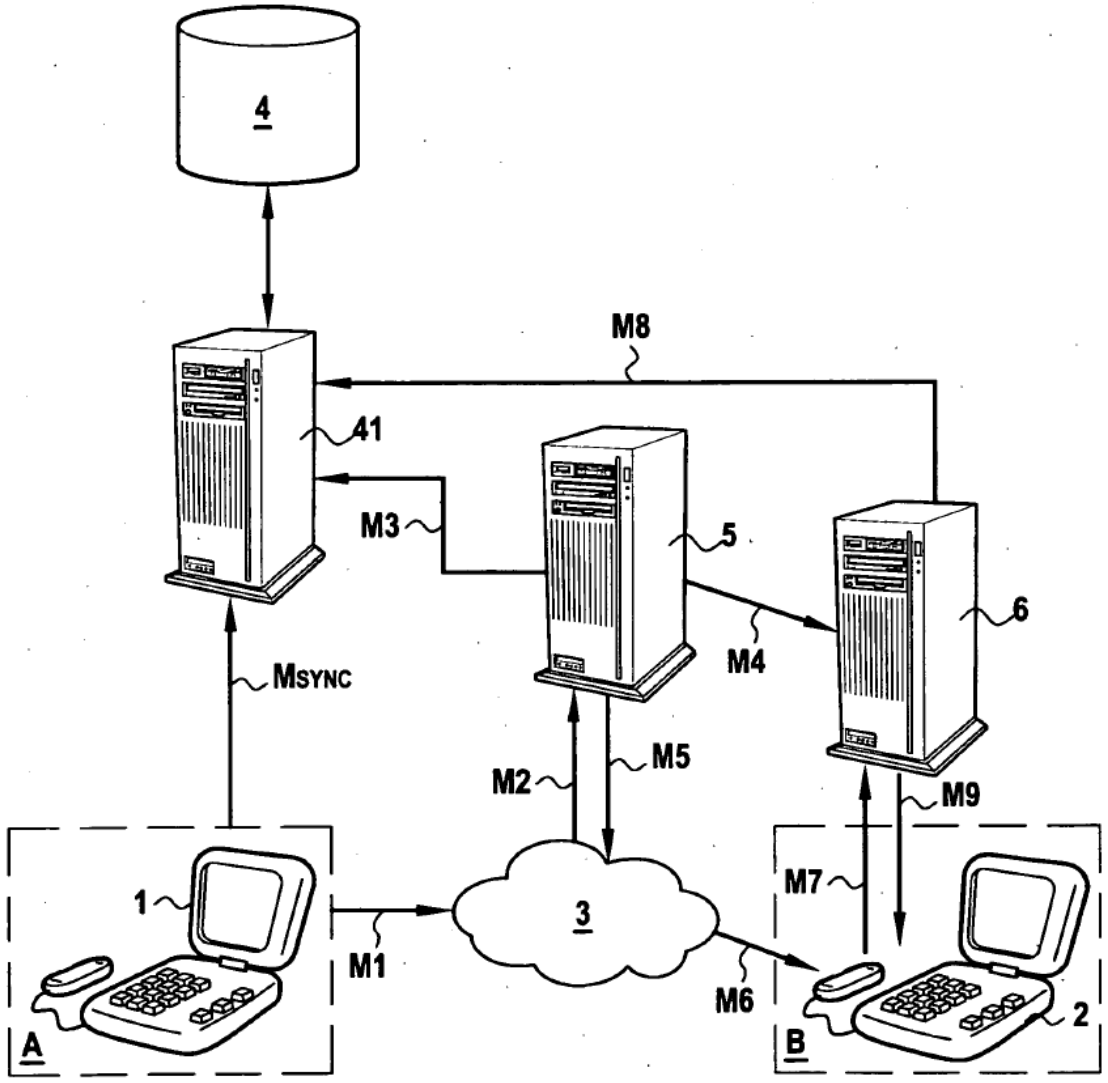

FIG.1

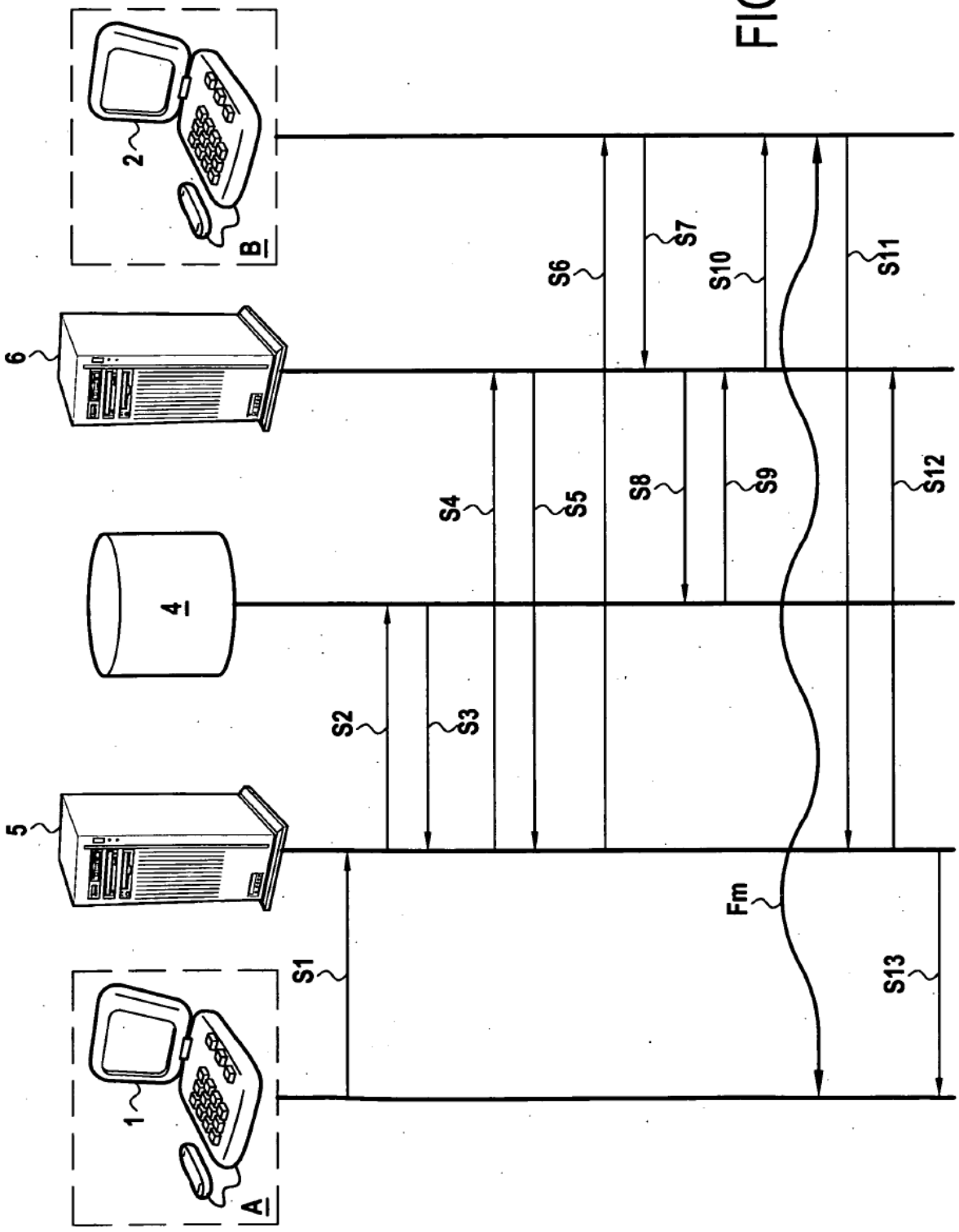

FIG.2

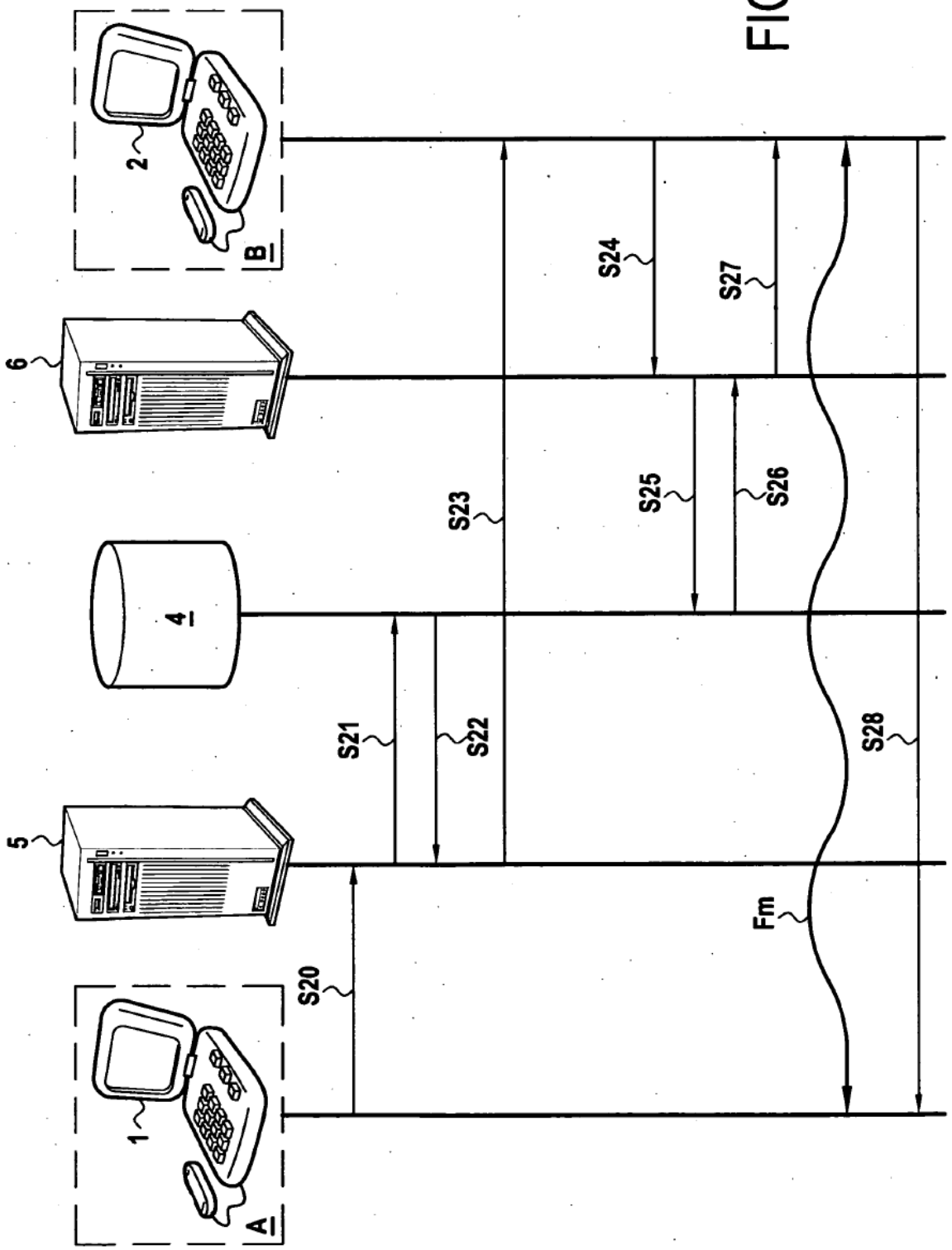

FIG.3

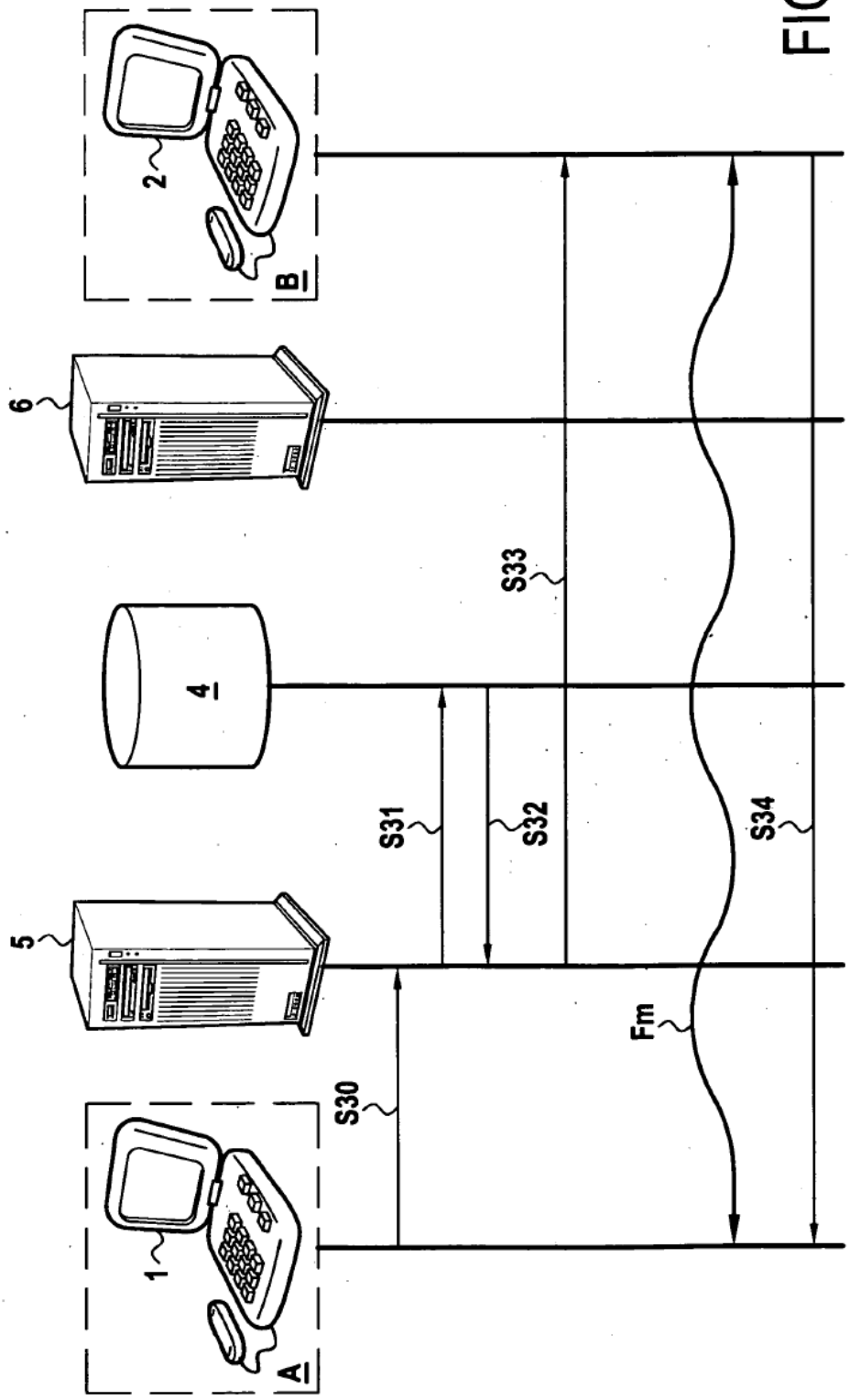

FIG.4