(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 469 871**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06T 1/00 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.04.2010 E 10159724 (3)**

(97) Fecha y número de publicación de la concesión europea: **12.03.2014 EP 2249543**

(54) Título: **Procedimiento para autorizar una conexión entre un terminal informático y un servidor de origen**

(30) Prioridad:

16.04.2009 FR 0901850

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.06.2014

(73) Titular/es:

SYNCHRONOSS TECHNOLOGIES FRANCE (100.0%)
Hôtel de Direction lot 101 102, 10 Place de la Joliette, Les Docks
13002 Marseille , FR

(72) Inventor/es:

COLON, FRANÇOIS

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

DESCRIPCIÓN

Procedimiento para autorizar una conexión entre un terminal informático y un servidor de origen.

La presente invención tiene por objetivo un procedimiento y un sistema que permita autorizar una conexión entre un terminal informático y un servidor de origen.

Campo técnico de la invención

La invención se refiere al campo técnico general de los protocolos que permiten proteger la autentificación del terminal informático frente de un servidor de origen.

La invención se aplica de manera preferida, pero no limitativa, a la autentificación de un usuario para: la apertura de una sesión de mensajería instantánea en el teléfono móvil, la activación de funcionalidades en un terminal móvil o fijo, la transmisión de datos en una red de comunicación segura (haciendo intervenir en particular unas tarjetas de chips), etc.

Estado de la técnica anterior

Los terminales informáticos (tales como los teléfonos móviles, ordenadores PC portátiles o fijos, PDA, BlackBerry®,…) están equipados generalmente con un cierto número de funcionalidades que permiten, por ejemplo, consultar unos correos electrónicos, abrir una sesión de mensajería instantánea, comunicar sobre un blog, transferir unos datos de seguridad, etc. Cada una de estas funcionalidades se implementa mediante una aplicación informática específica (o software) integrado en el terminal informático.

Cuando un usuario desea por ejemplo conectarse a un servicio de mensajería instantánea, la aplicación informática de su terminal emite una solicitud pidiendo al servidor establecer una conexión.

Es conocida una técnica de autentificación trivial en la que, para autorizar una conexión y activar una funcionalidad, el terminal informático debe transmitir inicialmente una palabra clave directamente al servidor de origen o a un servidor de pasarela (más conocido por el experto en la técnica con el término inglés “Gateway”) dispuesto entre dicho terminal y dicho servidor distante.

Por “palabra clave”, se entiende en el sentido de la presente invención, un código secreto asociado eventualmente al identificador del usuario.

En el caso en que la palabra clave se transmite previamente al servidor de pasarela, este último analiza dicha palabra clave y, en caso de autentificación, autoriza la conexión. Una vez que se ha establecido la conexión entre el terminal informático y el servidor de pasarela, este último se conecta al servidor de origen de manera que las informaciones con destino en, o emitidas por, dicho terminal transitan por dicho servidor de pasarela.

En el caso en que la palabra clave se transmite directamente al servidor de origen, este último verifica la palabra clave recibida y autoriza la conexión con el terminal si dicha palabra clave se autentifica.

Hasta el momento, las palabras clave se registran generalmente en los terminales informáticos y en los servidores distantes o de los servidores de pasarela.

El principal inconveniente ligado a este estado de las cosas es que un defraudador podría introducirse fácilmente en un terminal informático y robar la palabra clave de un usuario con el fin de hacerse pasar ilegalmente por él. Si los servidores distantes pueden ser en general difícilmente pirateados, no ocurre lo mismo con los servidores de pasarela. Estos últimos están en efecto sensiblemente menos protegidos que los servidores distantes y en caso de ataque, un defraudador podría sustraer el conjunto de las palabras clave de los usuarios con el fin de hacerse pasar ilegalmente por uno de entre ellos.

El documento JP 2005/293156, del 20 de octubre de 2005 (2005-10-20) describe un procedimiento de autentificación entre un terminal y un servidor distante. Este procedimiento comprende una etapa de intercambio del identificador y de la palabra clave entre el terminal y el servidor distante.

El problema técnico principal que viene a resolver la invención es mejorar la seguridad de los procedimientos de autorización de conexión entre un terminal informático y un servidor de origen.

Exposición de la invención

La invención viene a remediar los problemas ligados a las dificultades técnicas encontradas en los mecanismos de autentificación y de identificación entre un terminal informático y un servidor de origen.

Más precisamente, la invención tiene por objetivo un procedimiento para autorizar una conexión entre un terminal informático y un servidor de origen, siendo dicho procedimiento del tipo conocido en la técnica anterior, es decir en el que:

- el terminal transmite una palabra clave al servidor de origen,
- el servidor de origen verifica la palabra clave para autorizar la conexión con el terminal.

En un primer caso en el que la palabra clave se transmite previamente al servidor de pasarela dispuesto entre el terminal informático y el servidor de origen, el procedimiento objetivo de la invención se distingue por el hecho de que en una fase de inicialización:

- el terminal se conecta al servidor de pasarela dispuesto entre dicho terminal y el servidor de origen,
- el servidor de pasarela transmite al terminal una clave secreta,
- el terminal guarda temporalmente la palabra clave en un archivo de datos aplicando un algoritmo de cifrado iniciado por la clave secreta, posteriormente elimina dicha clave secreta y dicha palabra clave con el fin de no conservar más que dicho fichero que contiene dicha palabra clave,
  y por el hecho de que en una fase de conexión:

  - el terminal transmite el fichero de datos que contiene la palabra clave al servidor de pasarela,
  - el servidor de pasarela extrae la palabra clave del fichero ejecutando un algoritmo de cifrado inverso iniciado por la clave secreta, y transmite al servidor de origen dicha palabra clave sin guardarla,
  - el servidor de origen analiza la palabra clave recibida y autoriza la conexión con el terminal si dicha palabra clave se autentifica.

En un segundo caso en el que la palabra clave se transmite directamente al servidor de origen, el procedimiento objetivo de la invención es notable por el hecho de que en una fase de inicialización:

- el terminal se conecta al servidor de origen,
- el servidor de origen transmite al terminal una clave secreta,
- el terminal guarda temporalmente la palabra clave en un fichero de datos aplicando un algoritmo de cifrado iniciado por la clave secreta, posteriormente elimina dicha clave secreta y dicha palabra clave con el fin de no conservar más que dicho fichero que contiene dicha palabra clave,
  y por el hecho de que en una fase de conexión:
- el terminal transmite el fichero de datos que contiene la palabra clave al servidor de origen,
- el servidor de origen extrae la palabra clave del fichero ejecutando un algoritmo de cifrado inverso iniciado por la clave secreta, analiza dicha palabra clave y autoriza la conexión con el terminal si dicha palabra clave se autentifica.

Tanto en el primer como en el segundo caso, la palabra clave ya no se almacena en el terminal informático, sino que se mantiene almacenada temporalmente en un fichero. Una vez borradas la clave secreta y la palabra clave, el terminal posee solamente una palabra clave cifrada. El objetivo por tanto se ha alcanzado: la palabra clave ya no está escrita en el terminal. Si un defraudador se introduce en el terminal informático, le será ahora muy difícil conocer el fichero en el que está guardada temporalmente la palabra clave e incluso si descubre este fichero, le será casi imposible encontrar dicha palabra clave puesto que no conocerá la clave secreta.

En lo que concierne al primer caso, el servidor de pasarela no guarda las palabras clave de los usuarios y no guarda en memoria más que la clave secreta.

Si un defraudador se introduce en el servidor de pasarela, ya no tendrá por tanto la posibilidad de sustraer las palabras clave.

En lo que concierne al segundo caso, si un defraudador intercepta el fichero que contiene la palabra clave antes de que alcance el servidor de origen, no tendrá la posibilidad de encontrar dicha palabra clave puesto que no conocerá la clave secreta.

Con referencia al primer caso, para asegurar el envío de la clave secreta en el transcurso de la fase de inicialización:

- el servidor de pasarela transmite previamente al terminal una clave secreta secundaria,
- el servidor de pasarela cifra la clave secreta utilizando un algoritmo de cifrado iniciado por la clave secundaria, posteriormente transmite dicha clave secreta cifrada al terminal,
- el terminal extrae la clave secreta ejecutando un algoritmo de cifrado inverso iniciado por la clave secundaria.

Con referencia al segundo caso y para asegurar el envío de la clave secreta en el transcurso de la fase de inicialización:

- el servidor de origen transmite previamente al terminal una clave secreta secundaria,
- el servidor de origen cifra la clave secreta utilizando un algoritmo de cifrado iniciado por la clave secundaria, posteriormente transmite dicha clave secreta cifrada al terminal,
- el terminal extrae la clave secreta ejecutando un algoritmo de cifrado inverso iniciado por la clave secundaria.

Para optimizar la seguridad del procedimiento según el primer o el segundo caso, la palabra clave se almacena temporalmente en un fichero de medios integrado en el terminal aplicando un algoritmo de esteganografía.

La invención se refiere igualmente a unos sistemas que permiten implementar el procedimiento objetivo de la invención, según el primer o el segundo caso.

Preferiblemente, el terminal informático es un teléfono móvil y el servidor de origen es un servidor de comunidad de mensajería instantánea.

Breve descripción de las figuras

Surgirán mejor otras ventajas y características de la invención con la lectura de la descripción de un modo de realización preferido a continuación, con referencia a los dibujos adjuntos, realizados a título de ejemplo indicativo y no limitativo y en los que:

- la figura 1 ilustra diferentes etapas de la fase de inicialización del procedimiento de acuerdo con la invención, en el primer caso en el que la palabra clave se transmite previamente a un servidor de pasarela dispuesto entre el terminal informático y el servidor de origen,
- la figura 2 ilustra diferentes etapas de la fase de inicialización, según una variante de realización, en el primer caso,
- la figura 3 ilustra diferentes etapas de la fase de conexión en el primer caso
- la figura 4 ilustra diferentes etapas de la fase de inicialización del procedimiento de acuerdo con la invención, en el segundo caso en el que la palabra clave se transmite directamente al servidor de origen,
- la figura 5 ilustra diferentes etapas de la fase de inicialización, según una variante de realización, en el segundo caso,
- la figura 6 ilustra diferentes etapas de la fase de conexión en el segundo caso,
- la figura 7 ilustra la inserción de una palabra clave en una imagen mediante esteganografía.

Para mayor claridad, los elementos idénticos o similares se referencian por unos signos de referencia idénticos en el conjunto de las figuras.

Descripción detallada del modo de realización

El procedimiento objetivo de la invención permite proteger la autentificación de un terminal informático frente a un servidor de origen con el fin de establecer una conexión entre dicho terminal y dicho servidor de origen.

Este procedimiento se utiliza de manera preferida, pero no limitativa, para la autentificación de un usuario para: la apertura de una sesión de mensajería instantánea en el teléfono móvil, la activación de funcionalidades en el terminal móvil o fijo, la transmisión de datos sobre una red de comunicación de seguridad (haciendo intervenir en particular unas tarjetas de chips), etc.

El terminal informático T utilizado para la implementación de la invención puede ser un terminal móvil tal como un teléfono móvil, un aparato del tipo asistente digital personal (PDA), un aparato del tipo BlackBerry®, o un terminal fijo tal como un ordenador PC. De una forma bien conocida para el experto en la técnica, el terminal T está equipado con un procesador, configurado para ejecutar uno o varios programas, subprogramas, microprogramas o cualquier otro tipo de software equivalente, con el fin de generar las diferentes etapas del protocolo de autentificación que se van a describir en detalle en lo que sigue de la descripción.

El terminal T integra igualmente un cierto número de aplicaciones informáticas (programas, subprogramas, microprogramas,…) que le permiten implementar las diferentes funcionalidades que integra: correos electrónicos, blogs, mensajería instantánea, transferencia segura de datos, etc.

Para implementar estas funcionalidades, es necesario que el usuario del terminal informático T se identifique frente al servidor de origen.

El servidor de origen SS consiste en un ordenador o un programa informático configurado para proponer ciertas funcionalidades (correos, blogs,…) y en particular unos servicios de mensajería instantánea, a un terminal T que se conecta a él. El servidor de origen SS se asocia preferiblemente a diferentes comunidades de mensajería instantánea. Se conecta a una red de comunicación (MSM®, Jabber®, Yahoo!®, u otras) habitualmente empleada para implementar las diferentes funcionalidades citadas anteriormente.

De una manera bien conocida, este servidor de origen SS integra unas aplicaciones informáticas y está equipado con un procesador configurado para ejecutar uno o varios programas, subprogramas, microprogramas o cualquier otro tipo de software equivalente, con el fin de generar las diferentes etapas del protocolo de autentificación que se va a describir en detalle en lo que sigue de la descripción.

Con referencia a las figuras adjuntas, el terminal informático T debe transmitir una palabra clave PWD al servidor de origen SS. Este último verifica entonces la palabra clave PWD para autorizar la conexión con el terminal T.

Se pueden presentar dos casos:

- o bien la palabra clave PWD se transmite a un servidor de pasarela SP o “gateway” antes de ser transmitida al servidor de origen SS (figura 1),

- o bien la palabra clave se transmite directamente al servidor de origen SS (figura 2).

Primer caso: la palabra clave PWD se transmite al servidor de pasarela SP antes de transmitirse al servidor de origen SS.

Con relación a las figuras 1 a 3, un servidor de pasarela SP independiente o no del servidor de origen SS se dispone entre dicho servidor de origen y el terminal informático T de manera que las informaciones con destino en, o emitidas por, dicho terminal transiten por dicho servidor de pasarela.

En la práctica, este servidor de pasarela SP, más conocido por los técnicos en la materia por el término inglés “gateway”, es un ordenador o un programa informático configurado para proponer ciertos servicios a los terminales informáticos de los usuarios que se conectan a él. El servidor de pasarela SP puede estar equipado principalmente de medios que le permitan generar una sesión de mensajería instantánea, filtrar unos mensajes y generar unas listas de contactos de un usuario.

Otros servicios tales como: previsión meteorológica, publicidad, juegos, mensajería de audio u otros pueden implementarse igualmente por el servidor de pasarela SP.

Este último permite desviar y/o añadir ciertas funcionalidades sin tener que modificar el servidor de origen SS. De una manera bien conocida, el servidor de pasarela SP integra unas aplicaciones informáticas y está equipado con un procesador configurado para ejecutar uno o varios programas, subprogramas, microprogramas o cualquier otro tipo de software equivalente, con el fin de generar las diferentes etapas del protocolo de autentificación que se van a describir en detalle en lo que sigue de la descripción.

Con referencia a la figura 1, en una fase de inicialización, el terminal T se conecta al servidor de pasarela SP transmitiendo a dicho servidor una solicitud de inicialización Req_{inic} con el fin de descargar los recursos de una aplicación informática asociada a una o varias funcionalidades que el usuario desea obtener. En respuesta a esta solicitud, el servidor de pasarela SP puede transmitir al terminal T, además de los recursos de la aplicación, una clave secreta PPH.

Esta última es propia de cada usuario: hay tantas claves secretas PPH como usuarios. En la práctica, el terminal T transmite un identificador al servidor de pasarela SP que de vuelta transmite la clave secreta PPH.

Este identificador puede ser por ejemplo un identificador específico de cada usuario o un código de conexión a una comunidad de mensajería instantánea. La solicitud de inicialización Req_{inic} y la clave secreta PPH transitan en el canal de transmisión (o en otro canal) que une el terminal T al servidor de pasarela SP.

La clave secreta PPH integra en principio un número aleatorio n. Este número n es en la práctica un número entero hexadecimal de varios bits generado por un generador de números pseudoaleatorios (PNRG) integrado en el servidor. La clave secreta PPH puede integrar igualmente un marcador de tiempo t. Es posible por ejemplo implementar el marcador t como un número hexadecimal incrementado con cada recepción de una solicitud de inicialización Req_{inic} (por lo tanto evolucionando en el tiempo). Sin embargo, son conocidas otras técnicas por el experto en la técnica para implementar el marcador t. En la práctica, el marcador de tiempo t corresponde a la fecha de creación del número aleatorio n. El número n y el marcador t sirven para incrementar la entropía (dificultad de falsificación) de la clave secreta PPH.

En una variante de realización cuyas etapas se ilustran en la figura 2, se utiliza una clave secreta secundaria $PPH_{Secundaria}$ suplementaria en el curso de la fase de inicialización. Después de que el terminal T se haya conectado al servidor de pasarela SP, dicho servidor genera no solamente la clave secreta PPH definida anteriormente, sino igualmente una clave secundaria.

Esta clave es propia de cada usuario y está asociada en la práctica a cada identificador de los usuarios. La clave secreta secundaria $PPH_{Secundaria}$ consiste en principio en un número entero hexadecimal de varios bits. La clave

secreta PPH así como la clave secreta secundaria $PPH_{Secundaria}$ se almacenan entonces en una base de datos del servidor de pasarela SP. El servidor de pasarela SP transmite a continuación al terminal T la clave secreta secundaria $PPH_{Secundaria}$.

Esta última puede por ejemplo ser añadida, al vuelo, en los recursos de la aplicación informática descargada por el usuario, en una zona precisa que conoce dicha aplicación. La clave secundaria $PPH_{Secundaria}$ podrá ser guardada temporalmente astutamente en el código compilado de la aplicación informática. Durante la primera ejecución, el terminal T transmite al servidor de pasarela SP una solicitud Req_{exe} solicitando a dicho servidor la clave secreta PPH. En respuesta, el servidor de pasarela SP cifra la clave secreta PPH utilizando un algoritmo de cifrado $AC_{PPHsecundaria}$ iniciado por la clave secreta secundaria $PPH_{Secundaria}$ y posteriormente transmite dicha clave secreta PPH cifrada al terminal T. Se puede por ejemplo emplear un algoritmo de cifrado del tipo RSA o DES, siendo el objetivo obtener una cadena de caracteres binarios en los que se disimule la clave secreta PPH. El terminal T puede entonces extraer la clave secreta PPH ejecutando un algoritmo de cifrado inverso $AC^{-1}_{PPHsecundaria}$ iniciado por la clave secundaria $PPH_{Secundaria}$.

Se asegura así mejor el intercambio de la clave secreta PPH.

De acuerdo con las figuras 1 y 2, desde que el terminal T dispone de la clave secreta PPH, almacena temporalmente la palabra clave PWD en un fichero de datos MS aplicando un algoritmo de cifrado AS_{PPH} ventajosamente iniciado por la clave secreta PPH. Para reforzar la seguridad del protocolo, a partir de que se efectúa el algoritmo de cifrado AS_{PPH}, el terminal T elimina la clave secreta PPH.

El algoritmo de cifrado AS_{PPH} es propio de cada clave secreta PPH y por tanto de cada usuario.

Según un modo preferido de realización, la palabra clave PWD se almacena temporalmente mediante esteganografía en un fichero de medios MS grabado en el terminal informático T. La esteganografía es una técnica que permite disimular una información (la palabra clave PWD) en un soporte (el fichero de medios MS) de manera que la presencia de la información en el soporte sea imperceptible (ni visualmente, ni de manera audible) y por lo tanto indetectable por una persona.

Sin embargo, se podrían utilizar otros algoritmos de cifrado conocidos para el experto en la técnica con el objetivo de disimular la palabra clave PWD en un fichero cualquiera de datos MS almacenado en el terminal informático T.

Se podrían emplear por ejemplo unos algoritmos de cifrado RSA y DES, siendo el objetivo obtener una cadena de caracteres binarios (fichero) en la que se disimule la palabra clave PWD.

En la presente invención, la palabra clave PWD corresponde a un código secreto asociado con el identificador del usuario que se puede presentar bajo la forma de un número hexadecimal de varios bits. El fichero de medios MS es de manera general un fichero binario que forma parte de los recursos de la aplicación informática asociada a una funcionalidad montada en el terminal informático T. Se trata en la práctica de un fichero de imagen (JPEG, MPEG,...), de un fichero de audio (MP3,...) o de un fichero de video (MPEG2, MPEG4,...). Puede tratarse por ejemplo de una imagen de fondo de pantalla, de un mensaje de bienvenida de audio o video. El caso en el que la palabra clave PWD se disimula en una imagen JPEG o MPEG se ilustra en la figura 7: si la imagen representa un árbol con unas hojas, la palabra clave PWD podrá estar almacenada en unos píxeles correspondientes a una de las hojas del árbol u otras, porque no se controla forzosamente el entorno en el que se guardará dicha palabra clave.

El algoritmo de esteganografía AS preferentemente utilizado es el del tipo que utiliza la técnica LSB (por “Least Significant Bit” en inglés). Este algoritmo consiste en reemplazar los bits de peso reducido de los octetos que codifican la intensidad luminosa de los píxeles de la imagen por los bits de la clave secreta. Modificando un bit de peso reducido, es posible modificar ligeramente la intensidad luminosa o el color de un píxel de la imagen. Esta ligera modificación es imperceptible para el ojo humano e indetectable cuando se analiza el conjunto de los octetos que codifican la intensidad luminosa de los píxeles de la imagen. Por ejemplo si la intensidad luminosa de los píxeles de la imagen se codifica por los octetos: 001-000-100-110-101 y la palabra clave PWD corresponde al número: 11111, entonces la imagen modificada se codificará por los octetos siguientes: 00<u>1</u>-00<u>1</u>-10<u>1</u>-11<u>1</u>-10<u>1</u>. Igualmente el algoritmo de esteganografía se puede utilizar para la disimulación de una palabra clave PWD en un fichero de video. En un fichero de audio, se puede guardar la información en unas variaciones imperceptibles de sus codificaciones mediante unos bits 30 reducidamente significativos. Evidentemente, se puede utilizar cualquier otro algoritmo de esteganografía conveniente para el experto en la técnica.

Una vez que la palabra clave PWD se guarda en el fichero MS, el terminal T elimina dicha palabra clave con el fin de no conservar más que dicho fichero. Este último puede almacenarse a continuación en una zona de memoria del terminal T. Incluso si el fichero MS es detectado por un defraudador que se introduce ilegalmente en el terminal T, no habrá prácticamente ninguna oportunidad de detectar la palabra clave PWD.

Con relación a la figura 3, cuando el usuario del terminal T desea abrir una sesión, una aplicación informática colocada en dicho terminal emite una solicitud de conexión Req_{conex} con destino en el servidor de pasarela SP que la

transmite directamente al servidor de origen SS: esta es la fase de conexión.

Antes de activar la o las funcionalidades, el servidor de origen SS debe autentificar al terminal T. Para hacer esto, envía al terminal T, a través del servidor de pasarela SP, una solicitud de autentificación Req_{autent}. Las solicitudes Req_{conex} y Req_{autent} transitan en los canales de transmisión (o en otros canales) que unen al terminal T, el servidor de pasarela SP y el servidor de origen SS.

Cuando el terminal T recibe la solicitud de autentificación Req_{autent}, transmite al servidor de pasarela SP el fichero de datos MS en el que se guarda la palabra clave PWD. Este último no transita por lo tanto más que entre el terminal T y el servidor de pasarela SP e incluso si el fichero MS es interceptado por un defraudador, este último no tendrá prácticamente ninguna oportunidad de detectar la palabra clave PWD.

Después de haber recibido el fichero MS, el servidor de pasarela SP extrae la palabra clave PWD ejecutando un algoritmo de cifrado inverso AS^{-1}_{PPH}. En la práctica, este algoritmo de cifrado inverso se inicia por la clave de seguridad PPH asociada al usuario del terminal T. El servidor de pasarela SP transmite entonces al servidor de origen SS la palabra clave PWD extraída del fichero MS. La palabra clave PWD no queda guardada en el servidor de pasarela SP sino que por el contrario se elimina instantáneamente a partir de su envío hacia el servidor de origen SS.

Incluso si se introduce ilegalmente un defraudador en el servidor de pasarela SP, no tendrá ninguna oportunidad de detectar la palabra clave PWD.

El servidor de origen SS analiza la palabra clave PWD recibida y si dicha palabra clave se autentifica, autoriza la conexión con el terminal T para activar la o las funcionalidades deseadas por el usuario. En caso contrario, se puede enviar un mensaje de error desde el servidor de origen SS hacia el terminal T.

Segundo caso: la palabra clave PWD se transmite directamente al servidor de origen SS.

Con relación a las figuras 4 a 6, el terminal informático T está en este caso directamente unido al servidor de origen SS. Con referencia a la figura 4, en una fase de inicialización, el terminal T se conecta al servidor de pasarela SP transmitiendo al servidor de origen SS una solicitud de inicialización Req_{inic} con el fin de descargar los recursos de una aplicación informática asociada a una o varias funcionalidades que el usuario desea obtener. En respuesta a esta solicitud, el servidor de origen SS puede transmitir al terminal T, además de los recursos de la aplicación, una clave secreta PPH. Esta clave secreta PPH es idéntica a la clave descrita anteriormente. La solicitud de inicialización Req_{inic} y la clave secreta PPH transitan en el canal de transmisión (o en otro canal) que une el terminal T al servidor de origen SS.

En una variante de realización cuyas etapas se ilustran en la figura 5, se utiliza una clave secreta secundaria $PPH_{Secundaria}$ suplementaria en el transcurso de la fase de inicialización. Después de que el terminal T se conecte al servidor de origen SS, dicho servidor genera no solamente la clave secreta PPH definida anteriormente, sino igualmente una clave secundaria. Esta última es propia de cada usuario y está asociada en la práctica a cada identificador de los usuarios. La clave secreta PPH así como la clave secreta secundaria $PPH_{Secundaria}$ se almacenan entonces en una base de datos del servidor de origen SS. El servidor de origen SS transmite a continuación al terminal T la clave secreta secundaria $PPH_{Secundaria}$. Esta última puede ser añadida por ejemplo, al vuelo, en los recursos de la aplicación informática descargada por el usuario, en una zona precisa que conoce dicha aplicación. La clave secundaria $PPH_{Secundaria}$ podrá ser guardada astutamente en un código compilado de la aplicación informática. Durante la primera ejecución, el terminal T transmite al servidor de origen SS una solicitud Req_{exe} solicitando a dicho servidor la clave secreta PPH. En respuesta, el servidor de origen SS cifra la clave secreta PPH utilizando un algoritmo de cifrado $AC_{PPHsecundaria}$ iniciado por la clave secundaria $PPH_{Secundaria}$ y posteriormente transmite dicha clave secreta PPH cifrada al terminal T. Se puede por ejemplo emplear un algoritmo de cifrado del tipo RSA o DES, siendo el objetivo obtener una cadena de caracteres binarios en los que se disimule la clave secreta PPH. El terminal T puede extraer entonces la clave secreta PPH ejecutando un algoritmo de cifrado inverso $AC^{-1}_{PPHsecundaria}$ iniciado por la clave secreta secundaria $PPH_{Secundaria}$. Se asegura así mejor el intercambio de la clave secreta PPH.

De la misma manera que se ha descrito anteriormente en relación al primer caso, desde que el terminal dispone de la clave secreta PPH, el terminal T guarda la palabra clave PWD en un fichero de datos MS aplicando un algoritmo de cifrado AS_{PPH} ventajosamente iniciado por la clave secreta PPH. Este algoritmo de cifrado AS_{PPH} es idéntico al descrito para el primer caso.

Una vez que está guardada la palabra clave PWD en el fichero de datos MS, el terminal T elimina dicha palabra clave con el fin de no conservar más que dicho fichero. Este último puede almacenarse a continuación en una zona de memoria del terminal T.

Con referencia a la figura 6, cuando el usuario del terminal T desea abrir una sesión, una aplicación informática colocada en dicho terminal emite una solicitud de conexión Req_{conex} con destino en el servidor de origen SS: ésta es

la fase de conexión. De vuelta, el servidor de origen SS envía al terminal T una solicitud de autentificación Req_{autent}.

Cuando el terminal T recibe esta solicitud de autentificación Req_{autent}, transmite al servidor de origen SS el fichero de datos MS en el que está guardada la palabra clave PWD. Esta última no transita por tanto más que entre el terminal T y el servidor de origen SS. Después de haber recibido el fichero MS, el servidor de origen SS extrae la palabra clave PWD ejecutando un algoritmo de cifrado inverso AS^{-1}_{PPH}, ventajosamente iniciado por la clave secreta PPH asociada al usuario del terminal T.

El servidor de origen SS analiza la palabra clave PWD recibida y si dicha palabra clave se autentifica, autoriza la conexión con el terminal T para activar la o las funcionalidades deseadas por el usuario. En caso contrario, se puede enviar un mensaje de error desde el servidor de origen SS hacia el terminal T.

REIVINDICACIONES

1. Procedimiento para autorizar una conexión entre un terminal informático (T) y un servidor de origen (SS), y en el que:

- el terminal (T) transmite una palabra clave (PWD) al servidor de origen (SS),
- el servidor de origen (SS) verifica la palabra clave (PWD) para autorizar la conexión con el terminal (T),

caracterizado por el hecho de que en una fase de inicialización:

- el terminal (T) se conecta a un servidor de pasarela (SP) dispuesto entre dicho terminal y el servidor de origen (SS),
- el servidor de pasarela (SP) transmite al terminal (T) una clave secreta (PPH),
- el terminal (T) guarda temporalmente la palabra clave (PWD) en un archivo de datos (MS) aplicando un algoritmo de cifrado (AS_{PPH}) iniciado por la clave secreta (PPH), posteriormente elimina dicha clave secreta y dicha palabra clave con el fin de no conservar más que dicho fichero que contiene dicha palabra clave,

y **por el hecho de que** en una fase de conexión:

- el terminal (T) transmite al servidor de pasarela (SP) el fichero de datos (MS) que contiene la palabra clave (PWD), siendo guardada dicha palabra clave (PWD) en el fichero de datos (MS) aplicando un algoritmo de esteganografía (AS_{PWD});
- el servidor de pasarela (SP) extrae la palabra clave (PWD) del fichero (MS) ejecutando un algoritmo de cifrado inverso (AS^{-1}_{PPH}) iniciado por la clave secreta (PPH), y transmite al servidor de origen (SS) dicha palabra clave sin guardarla,
- el servidor de origen (SS) analiza la palabra clave (PWD) recibida y autoriza la conexión con el terminal (T) si dicha palabra clave se autentifica.

2. Procedimiento según la reivindicación 1, en el que en el transcurso de la fase de inicialización:

- el servidor de pasarela (SP) transmite previamente al terminal (T) una clave secreta secundaria ($PPH_{Secundaria}$),
- el servidor de pasarela (SP) cifra la clave secreta (PPH) utilizando un algoritmo de cifrado ($AC_{PPHsecundaria}$) iniciado por la clave secundaria ($PPH_{Secundaria}$), posteriormente transmite dicha clave secreta (PPH) cifrada al terminal (T),
- el terminal (T) extrae la clave secreta (PPH) ejecutando un algoritmo de cifrado inverso ($AC^{-1}_{PPHsecundaria}$) iniciado por la clave secundaria ($PPH_{Secundaria}$).

3. Procedimiento para autorizar una conexión entre un terminal informático (T) y un servidor de origen (SS), y en el que:

- el terminal (T) transmite una palabra clave (PWD) al servidor de origen (SS),
- el servidor de origen (SS) verifica la palabra clave (PWD) para autorizar la conexión con el terminal (T),

caracterizado por el hecho de que en una fase de inicialización:

- el terminal (T) se conecta al servidor de origen (SS),
- el servidor de origen (SS) transmite al terminal (T) una clave secreta (PPH),
- el terminal (T) guarda temporalmente la palabra clave (PWD) en un archivo de datos (MS) aplicando un algoritmo de cifrado (AS_{PPH}) iniciado por la clave secreta (PPH), posteriormente elimina dicha clave secreta y dicha palabra clave con el fin de no conservar más que dicho fichero que contiene dicha palabra clave,

y **por el hecho de que** en una fase de conexión:

- el terminal (T) transmite al servidor de origen (SS) el fichero de datos (MS) que contiene la palabra clave (PWD), siendo guardada dicha palabra clave (PWD) en el fichero de datos (MS) aplicando un algoritmo de esteganografía (AS_{PWD});
- el servidor de origen (SS) extrae la palabra clave (PWD) del fichero (MS) ejecutando un algoritmo de cifrado inverso (AS^{-1}_{PPH}) iniciado por la clave secreta (PPH), analiza dicha palabra clave y autoriza la conexión con el terminal (T) si dicha palabra clave se autentifica.

4. Procedimiento según la reivindicación 3, en el que en el transcurso de la fase de inicialización:

- el servidor de origen (SS) transmite previamente al terminal (T) una clave secreta secundaria ($PPH_{Secundaria}$),
- el servidor de origen (SS) cifra la clave secreta (PPH) utilizando un algoritmo de cifrado ($AC_{PPHsecundaria}$) iniciado por la clave secundaria ($PPH_{Secundaria}$), posteriormente transmite dicha clave secreta (PPH) cifrada al terminal (T),
- el terminal (T) extrae la clave secreta (PPH) ejecutando un algoritmo de cifrado inverso ($AC^{-1}_{PPHsecundaria}$)

iniciado por la clave secundaria ($PPH_{Secundaria}$).

5. Sistema para autorizar una conexión entre un terminal informático (T) y un servidor de origen (SS), y en el que:

- el terminal (T) comprende un medio para transmitir una palabra clave (PWD) al servidor de origen (SS),
- el servidor de origen (SS) comprende un medio para verificar la palabra clave (PWD) para autorizar la conexión con el terminal (T),

caracterizado por el hecho de que en una fase de inicialización:

- el terminal (T) comprende un medio para conectarse a un servidor de pasarela (SP) dispuesto entre dicho terminal y el servidor de origen (SS),
- el servidor de pasarela (SP) comprende un medio para transmitir al terminal (T) una clave secreta (PPH),
- el terminal (T) comprende un medio para guardar temporalmente la palabra clave (PWD) en un archivo de medios (MS) aplicando un algoritmo de cifrado (AS_{PPH}) iniciado por la clave secreta (PPH), y un medio para eliminar dicha clave secreta y dicha palabra clave con el fin de no conservar más que dicho fichero que contiene dicha palabra clave,

y **por el hecho de que** en una fase de conexión:

- el terminal (T) comprende un medio para transmitir el fichero de medios (MS) que contiene la palabra clave (PWD) al servidor de pasarela (SP),
- el servidor de pasarela (SP) comprende un medio para extraer la palabra clave (PWD) del fichero de medios (MS) ejecutando un algoritmo de cifrado inverso (AS^{-1}_{PPH}) iniciado por la clave secreta (PPH), y un medio para transmitir al servidor de origen (SS) dicha palabra clave sin guardarla,
- el servidor de origen (SS) comprende un medio para analizar la palabra clave (PWD) recibida y autorizar la conexión con el terminal (T) si dicha palabra clave se autentifica.

6. Sistema para autorizar una conexión entre un terminal informático (T) y un servidor de origen (SS), y en el que:

- el terminal (T) comprende un medio para transmitir una palabra clave (PWD) al servidor de origen (SS),
- el servidor de origen (SS) comprende un medio para verificar la palabra clave (PWD) para autorizar la conexión con el terminal (T),

caracterizado por el hecho de que en una fase de inicialización:

- el terminal (T) comprende un medio para conectarse a un servidor de origen (SS),
- el servidor de origen (SS) comprende un medio para transmitir al terminal (T) una clave secreta (PPH),
- el terminal (T) comprende un medio para guardar temporalmente la palabra clave (PWD) en un archivo de medios (MS) aplicando un algoritmo de cifrado (AS_{PPH}) iniciado por la clave secreta (PPH), y un medio para eliminar dicha clave secreta y dicha palabra clave con el fin de no conservar más que dicho fichero de medios que contiene dicha palabra clave,

y **por el hecho de que** en una fase de conexión:

- el terminal (T) comprende un medio para transmitir el fichero de medios (MS) que contiene la palabra clave (PWD) al servidor de origen (SS),
- el servidor de origen (SS) comprende un medio para extraer la palabra clave (PWD) del fichero (MS) ejecutando un algoritmo de cifrado inverso (AS^{-1}_{PPH}) iniciado por la clave secreta (PPH), un medio para analizar dicha palabra clave y autorizar la conexión con el terminal (T) si dicha palabra clave se autentifica.

7. Sistema según una de las reivindicaciones 5 o 6, en el que el terminal informático (T) es un teléfono móvil.

8. Sistema según una de las reivindicaciones 5 a 7, en el que el servidor de origen (SS) es un servidor de comunidad de mensajería instantánea.

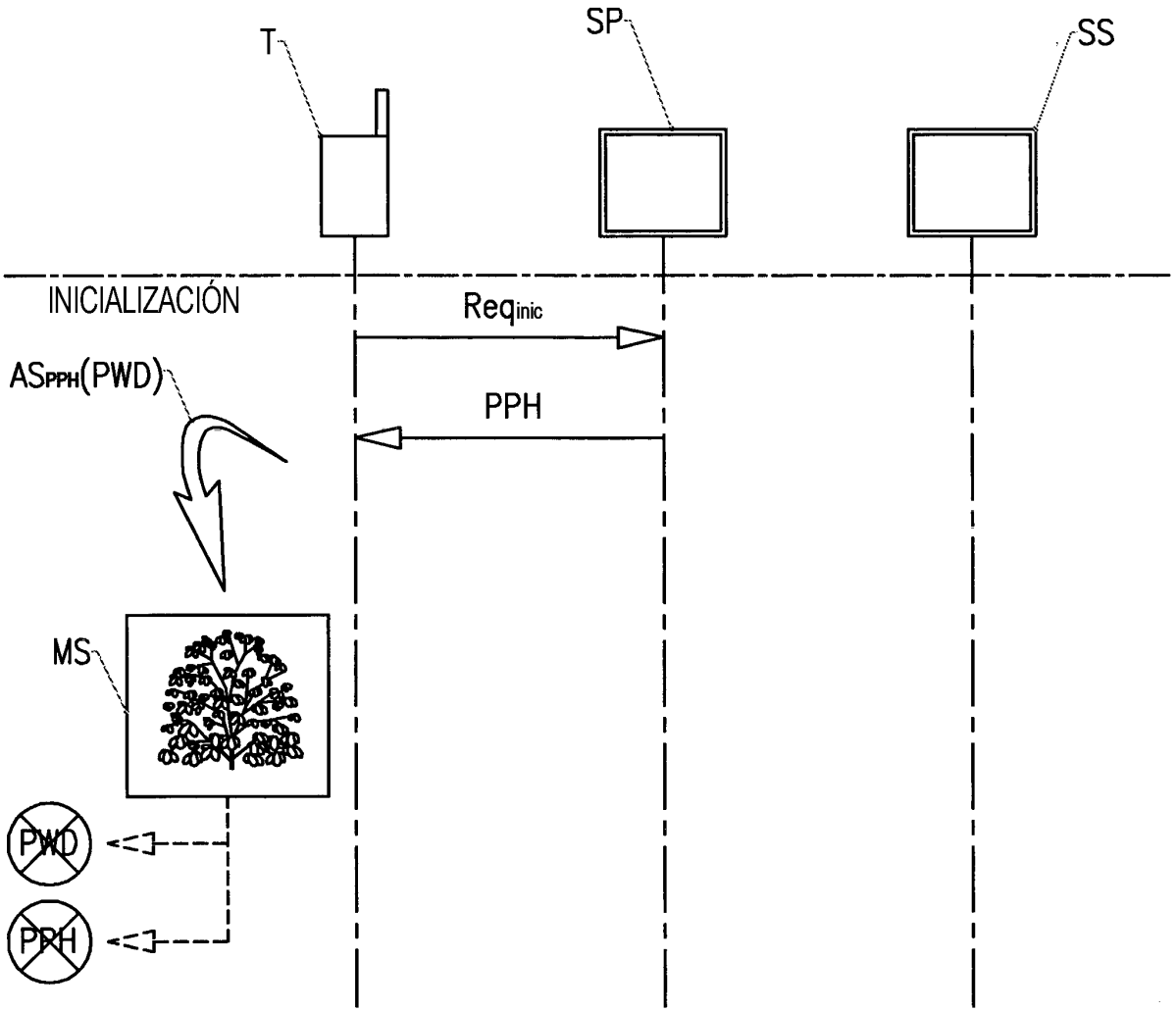

Fig. 1

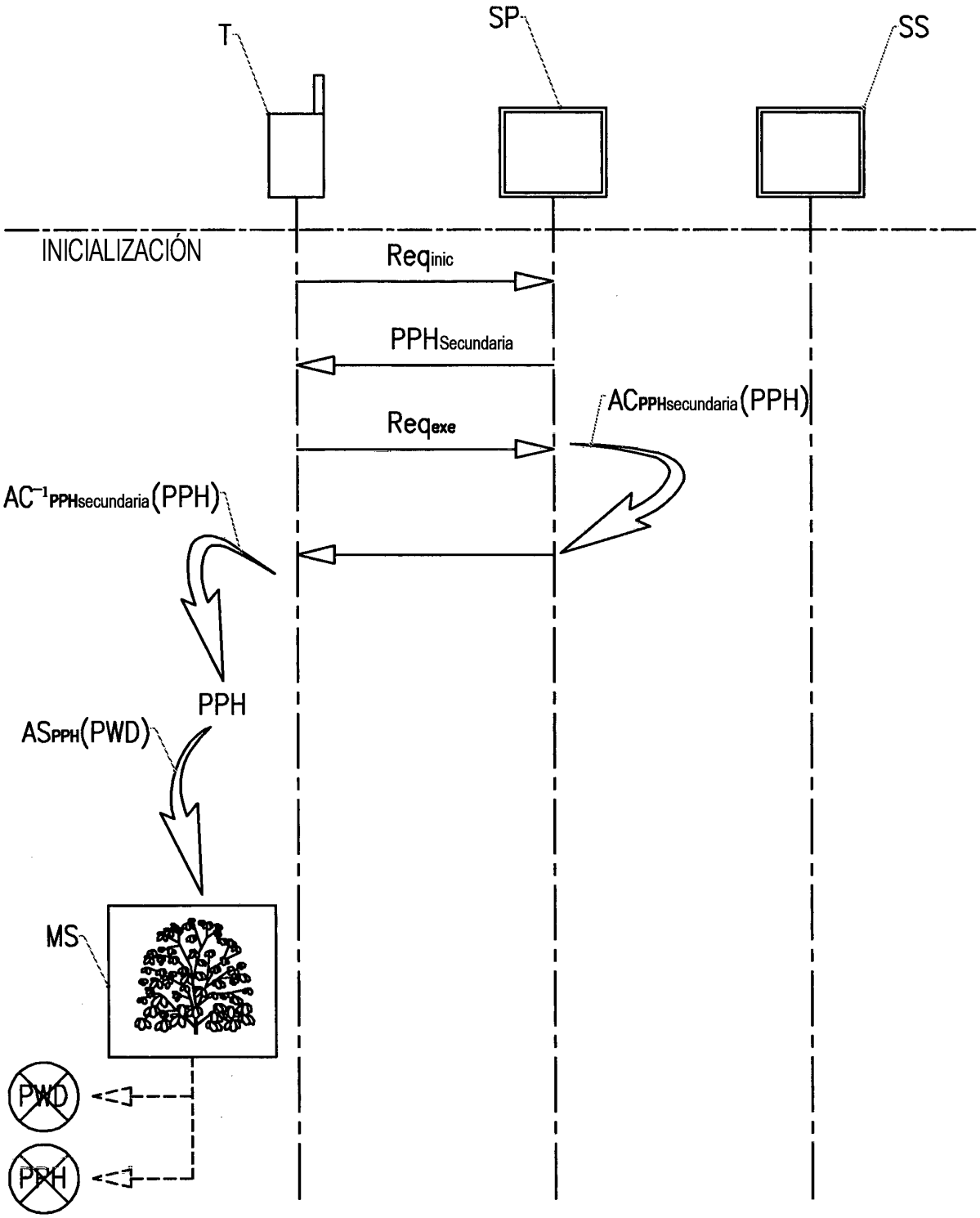
T
SP
SS
INICIALIZACIÓN
Req inic
PPH Secundaria
AC PPH secundaria (PPH)
Req exe
AC⁻¹ PPH secundaria (PPH)
PPH
AS PPH (PWD)
MS
PWD
PPH

Fig. 2

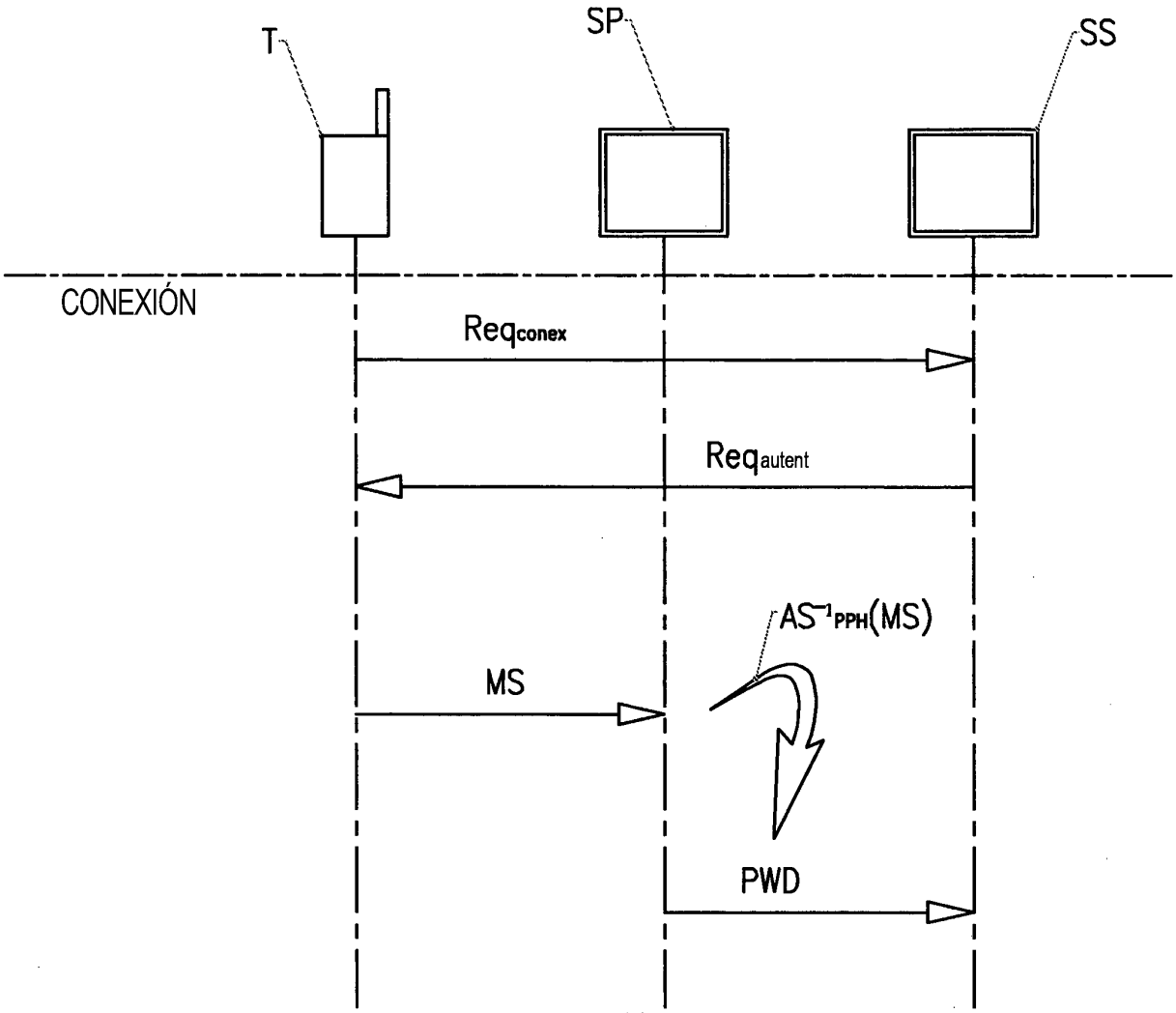

Fig. 3

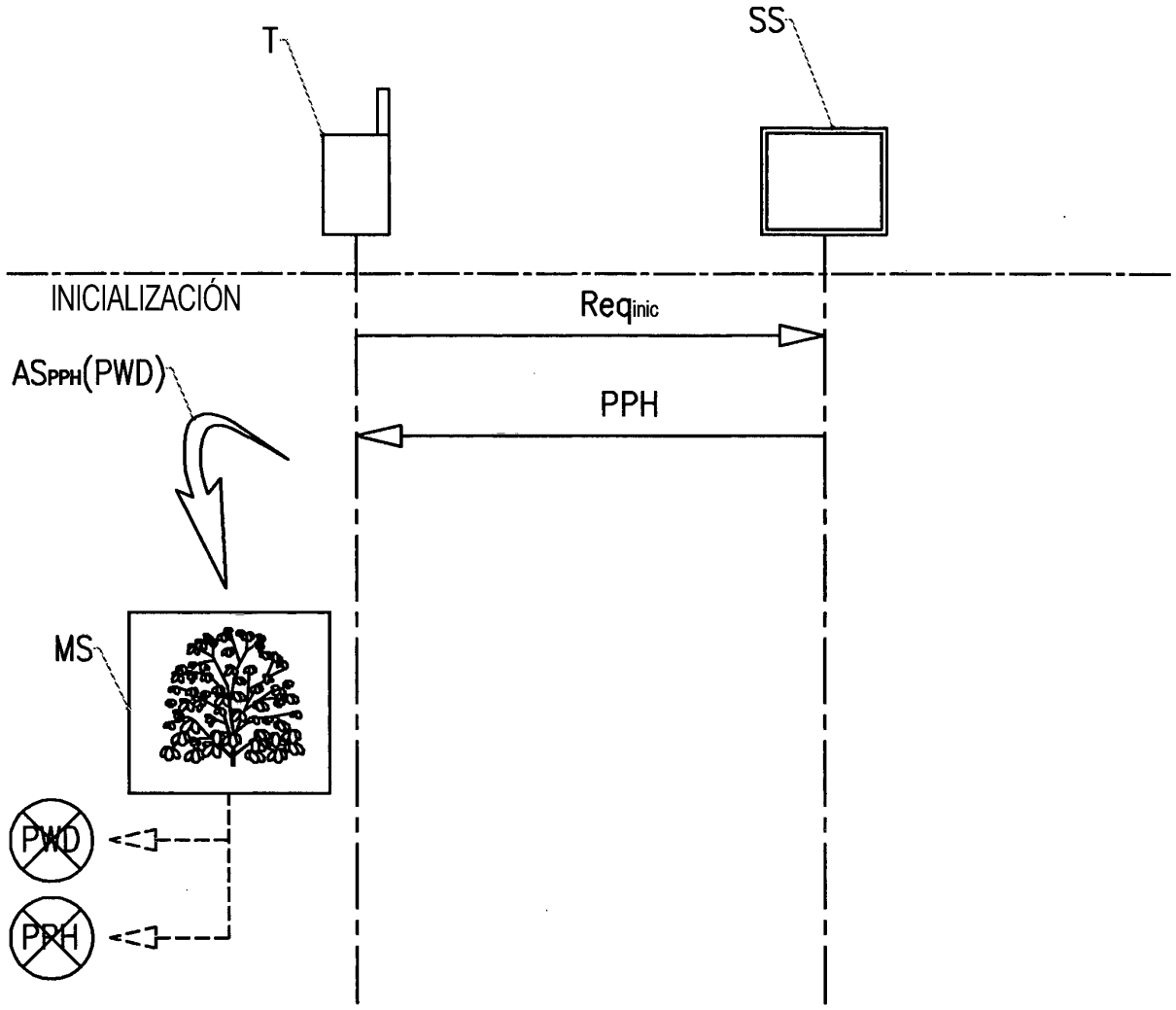

Fig. 4

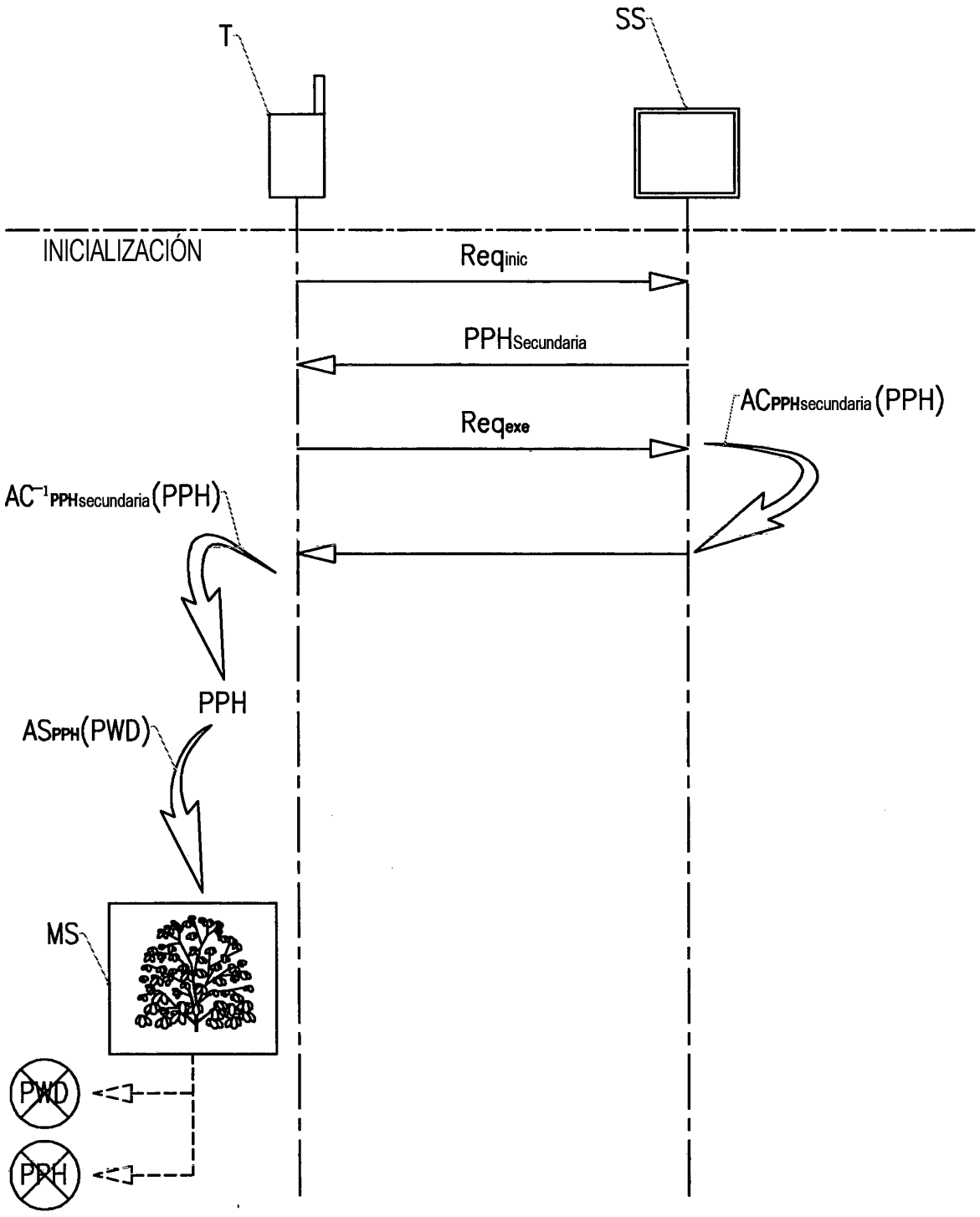
T
SS
INICIALIZACIÓN
Reqinic
PPHSecundaria
ACPPHsecundaria(PPH)
Reqexe
AC-1PPHsecundaria(PPH)
PPH
ASPPH(PWD)
MS
PWD
PPH

Fig. 5

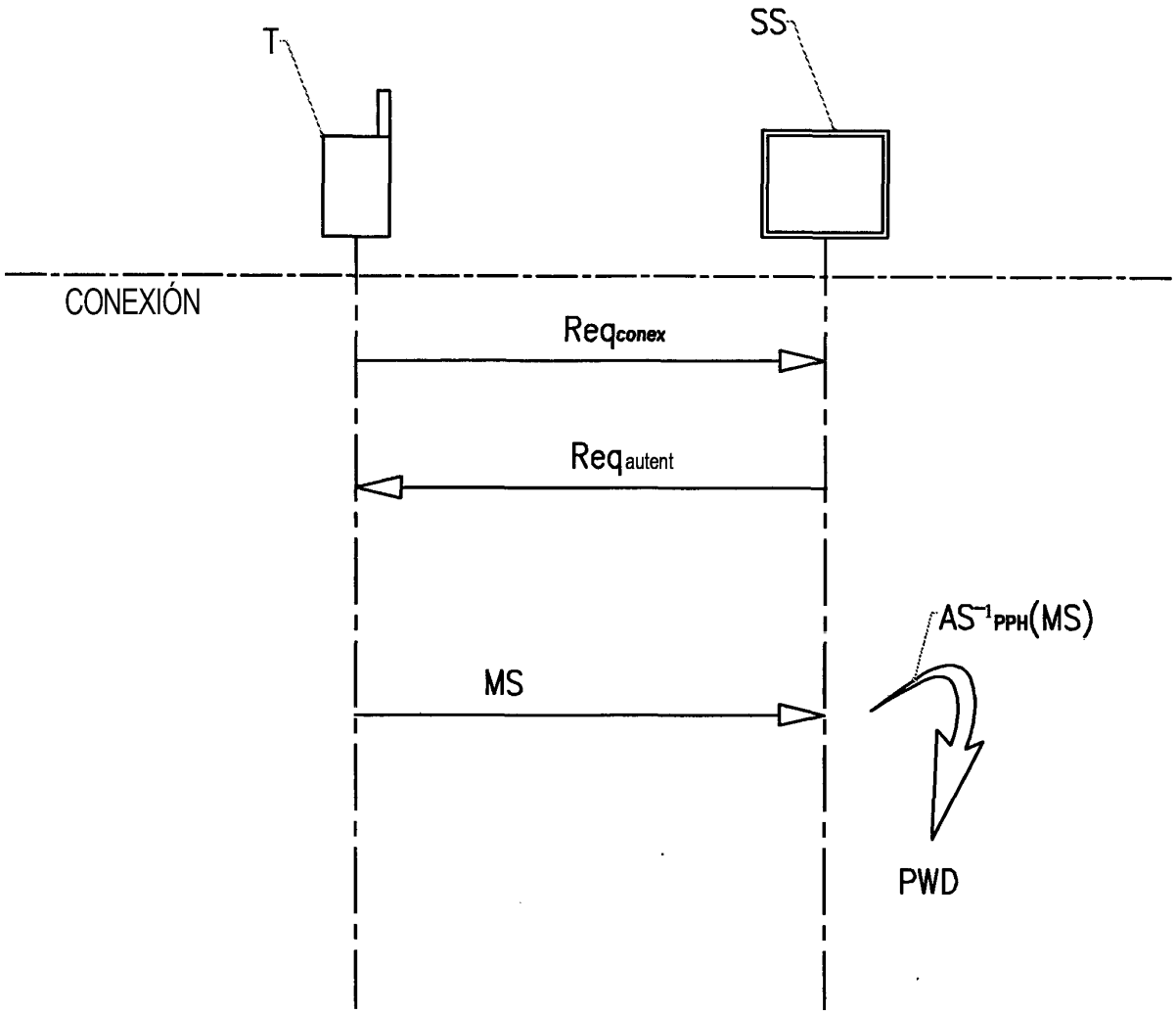

Fig. 6

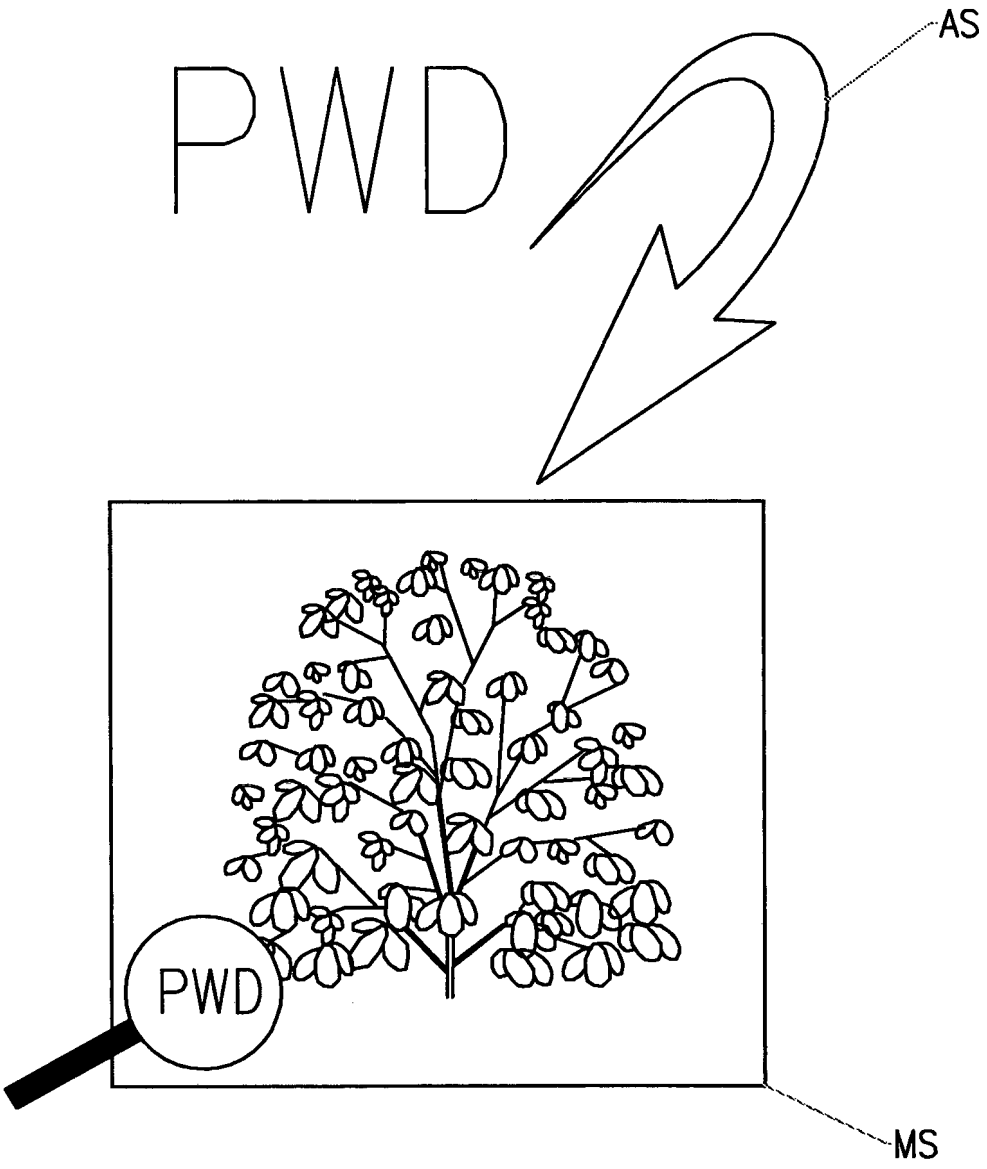

Fig. 7