(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 407 147**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.08.2007 E 07788516 (8)**

(97) Fecha y número de publicación de la concesión europea: **13.02.2013 EP 2055064**

(54) Título: **Sistema y procedimiento de gestión descentralizada de un sistema seguro que proporciona diferentes servicios**

(30) Prioridad:

23.08.2006 FR 0607469

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.06.2013

(73) Titular/es:

THALES (100.0%)
45 RUE DE VILLIERS
92200 NEUILLY SUR SEINE, FR

(72) Inventor/es:

ROUSSET, GILLES

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Sistema y procedimiento de gestión descentralizada de un sistema seguro que proporciona diferentes servicios

El objeto de la invención se refiere a un procedimiento y a un sistema que permite que un tercero de confianza gestione de manera descentralizada un sistema seguro.

La invención se aplica, en particular, en cualquier sistema de comunicación o informático que ofrece unos servicios de libre acceso para el público en general y unos servicios accesibles a través de una clave de acceso o de un código.

La invención se puede utilizar, en particular, en los sistemas de posicionamiento por satélite.

Un sistema seguro que proporciona diferentes servicios accesibles a través de claves y unas señales accesibles para el público en general comprende, por lo general, un servicio de gestión centralizado. Los receptores que se pueden utilizar para acceder al sistema de pago o servicios regulados (es necesario disponer de las claves) los gestionan el operador responsable de la infraestructura del sistema. La gestión de los receptores se centraliza por tanto en la infraestructura con una capacidad limitada de ancho de banda que solo permite gestionar un número limitado de usuarios de los servicios regulados. Además, en aras de la optimización, los usuarios se agrupan en « grupo de usuarios » que comparten las mismas características y que deben someterse a las mismas restricciones decididas de manera centralizada. Asimismo, por el carácter centralizado de la gestión, los tiempos de respuesta de la infraestructura son elevados, en particular para el acceso de los abonados al servicio, así como para la retirada de su derecho.

Por último, teniendo en cuenta los principios de gestión de los abonados que se aplican, la denegación de un usuario, acción que permite suprimir de manera temporal el acceso de un usuario a un servicio determinado, puede interferir con otros usuarios, privándolos por tanto de forma temporal del acceso al servicio.

En el documento titulado « IBM Cryptolopes, Superdistribution and Digital Rights Management », XP002132994, el « publisher » distribuye la criptología que se cifra de manera centralizada. La infraestructura proveedora de servicios no transmite directamente la señal ni las claves de denegación hacia los usuarios y no recibe la señal de la infraestructura ni las claves de denegación de la infraestructura.

La invención se refiere a un sistema para gestionar la distribución de claves de acceso a los servicios ofrecidos por una infraestructura de una manera descentralizada de acuerdo con la reivindicación 1.

Los medios de distribución de las claves entre un receptor maestro y un receptor esclavo comprenden, por ejemplo, una conexión segura y una conexión no segura.

El sistema puede ser un sistema de posicionamiento por satélite y en el que los servicios son la información de navegación.

La invención también se refiere a un procedimiento de gestión descentralizada de un sistema seguro de acuerdo con la reivindicación 4.

Los servicios son, por ejemplo, unos servicios de navegación y la transmisión de las señales se lleva a cabo por satélite.

Se puede utilizar una conexión segura para transmitir la clave de base.

El sistema y el procedimiento de acuerdo con la invención ofrecen en particular las siguientes ventajas: permiten una gestión descentralizada, individualizada y autónoma de grupos de usuarios de un servicio regulado por una entidad abonada a los servicios de la infraestructura del tercero de confianza y que se basa en una red de comunicación.

Se mostrarán mejor otras características y ventajas de la presente invención con la lectura de la siguiente descripción, que se da a título ilustrativo y en modo alguno limitativo, que lleva adjuntas unas figuras que representan:

- la figura 1 una estructura de acuerdo con la técnica anterior de un sistema seguro que ofrece varios servicios;
- la figura 2 una arquitectura de sistema de acuerdo con la invención.

En la figura 1 se ha representado una arquitectura de sistema de acuerdo con la técnica anterior.

Esta comprende una infraestructura proveedora de servicios 1 que proporciona las señales y/o los servicios cifrados y las actualizaciones de las claves de acceso o señal y/o a los servicios. Un centro de gestión centralizado 2 está adaptado para recoger las necesidades de cada usuario abonado y las transmite a la infraestructura que va a emitir las señales y las claves o denegación. El centro de gestión conocido por el experto en la materia permite, en particular, que el solicitante gestione la asignación de los derechos a sus usuarios; derechos obtenidos a partir de la gestión centralizada de la infraestructura proveedora de servicios.

En función de las informaciones recibidas, la infraestructura proporciona, a un grupo de usuarios o abonados, la señal que contiene en particular las claves de descifrado necesarias que permiten el acceso a los servicios seguros por un periodo de tiempo determinado o la información de denegación para los usuarios que ya no tienen el derecho de acceder a un determinado servicio.

Los usuarios se agrupan en « grupo de usuarios » que comparten las mismas características y que deben someterse a las mismas restricciones decididas de manera centralizada.

A los usuarios se les proporcionan unos medios de recepción, denominados receptor esclavo 3 en la figura. Estos medios comprenden un módulo 4 adaptado para extraer una parte de las claves, y un módulo de descifrado o decodificación 5 adaptado para descifrar la señal y/o los servicios.

Teniendo en cuenta los principios de gestión de los abonados que se aplican, la denegación de un usuario puede interferir con otros usuarios, privándolos por tanto de manera temporal del acceso al servicio.

La figura 2 representa un ejemplo de arquitectura de sistema de acuerdo con la invención que se basa en una infraestructura proveedora de servicios 10, un centro de gestión centralizado de las comunicaciones y de gestión de las claves 11, que comprende, por ejemplo, un receptor maestro 12.

La infraestructura proveedora de servicios comprende diferentes medios (no representados en la figura) adaptados en particular para generar una señal y/o unos servicios cifrados y para llevar a cabo las actualizaciones de las claves de acceso a la señal y/o a los servicios o también a la información de denegación.

El centro de comunicación centralizado 11 está compuesto por unos módulos adaptados para ejecutar las siguientes funciones:

Un módulo 13 adaptado para la gestión de los derechos de los usuarios (asociación receptor-derechos), situado en una interfaz hombre máquina, por ejemplo un ordenador;

En el receptor maestro 12:

- un módulo 14 adaptado para la gestión de los receptores esclavos (asociación receptor-usuario);
- un módulo 15 adaptado para la recepción y la extracción de los derechos, dando estos derechos acceso a los servicios gestionados de manera centralizada en la infraestructura;
- un módulo 16 para la gestión de las claves;
- un módulo 17 de gestión de la distribución individualizada de los derechos a los receptores.

Estas funciones permiten garantizar la seguridad permanente del servicio al cual dan acceso los derechos. Sin salirse del marco de la invención, el receptor maestro puede comprender otras funciones cuya gestión está garantizada por el centro de gestión. Estas funciones permiten de este modo ampliar el número de servicios controlados por el centro de gestión y a los que el receptor esclavo se puede abonar mediante la distribución individualizada de los derechos.

El receptor « maestro » 12 integra todas las funciones de seguridad y actúa como retransmisor inteligente frente a los receptores denominados « esclavos » 18. Este recibe una señal de la infraestructura, así como las claves de autorización de acceso a un servicio para un usuario determinado.

Los receptores « esclavos » integran únicamente la función de adquisición de la señal de servicio regulado S. Un receptor esclavo recibe una señal y unas claves o una denegación de la parte de la infraestructura proveedora de servicios. Este comprende un medio 19 adaptado para la extracción de una parte de las claves recibidas de la infraestructura y un medio 20 adaptado para descifrar la señal y/o los servicios. Los receptores esclavos están controlados por el receptor « maestro » mediante un sistema seguro de distribución de claves 21, 22.

El sistema de gestión local del receptor maestro permite el funcionamiento del receptor esclavo por un periodo determinado distribuyéndoles unas claves que se pueden gestionar en el sistema de gestión y de supervisión del receptor « maestro ».

Se dan a continuación los detalles de las funciones de comunicación:

Extracción de los derechos asociados a un servicio. Esta función está garantizada por el receptor maestro que es un abonado de la infraestructura (declarado en la infraestructura) y, como tal, recibe la señal de servicio S difundida por los sistemas de emisión de mensajes y de informaciones de la infraestructura.De la señal recibida, el receptor maestro extrae los servicios que, en el caso de un sistema de posicionamiento por satélite, son por ejemplo:

- información de navegación (almanaque, datos de integridad, etc.); y
- derechos del servicio, es decir, los derechos vinculados a un usuario.

Estos derechos están contenidos en un mensaje de seguridad del servicio que el « receptor maestro » descifra. De este extrae un sistema de claves con una validez espacio-temporal que se difundirán por completo o en parte a los receptores esclavos, permitiéndoles de este modo acceder a la señal de servicio.

Gestión local de los receptores.

La gestión local de los receptores garantiza la gestión del conjunto de receptores esclavos, la extracción y la asignación de claves a estos receptores esclavos. El sistema de gestión local de los usuarios comprende, por ejemplo, un medio adaptado para apropiarse de los derechos de servicio adquiridos por el receptor maestro y los distribuye de forma limitada a los receptores « esclavo ».

En el centro de gestión, la función de gestión « esclavo » permite el registro, la gestión de los derechos y la anulación de los receptores esclavos que tiene vinculados. Declarar un receptor esclavo consiste en identificarlo, asignarle una autonomía (p. ej. una duración y/o un espacio físico de acceso a la señal de servicio sin comunicación con el centro de gestión local). Utilizando esta información diversa, esta función dirige la función de gestión de las claves para inicializar el receptor esclavo y a continuación permitir la recepción regular de sus derechos.

La función gestión de clave permite gestionar unas claves de base, y cifrar unas claves de servicio mediante la clave de base de los receptores. Esta clave oculta, distribuida de manera regular a los receptores esclavos, constituye sus derechos para acceder a la señal de servicio a petición de la función de gestión de los usuarios, la función de gestión de las claves:

- genera unas claves de base durante la declaración de un nuevo receptor;
- programa el cifrado de claves con una frecuencia dictada por la autonomía deseada para los receptores esclavos.

La función « distribución de claves » garantiza la distribución de las claves de base y de los derechos de los receptores esclavos (claves de servicio cifradas mediante la clave base).

Las claves de base son extremadamente sensibles y se transfieren, por ejemplo, a los receptores esclavos utilizando una red protegida. Los receptores esclavos tienen acceso a esta red protegida cada vez que comienzan su misión (y, por lo tanto, se encuentran próximos a una infraestructura protegida).

Las claves ocultas (los derechos de usuarios S) no son sensibles ya que están protegidas por la clave de base de los receptores « esclavos ». Estas claves se distribuyen a los receptores esclavos por una red poco segura con una frecuencia en función de la autonomía otorgada a los receptores esclavos.

El sistema de gestión local comprende, en particular, un dispositivo de generación y a continuación de cifrado de claves, así como un dispositivo de distribución de estas claves por dos canales diferentes, respectivamente 18 y 19 en la figura 2, por ejemplo:

- una red muy segura para transmitir las claves de base a los receptores esclavos; y
- una red de comunicación/distribución con una baja protección de privacidad para la gestión de derechos de los receptores « esclavo ».

Imaginemos que el receptor maestro adquiere los derechos, que le permiten acceder a la señal de servicio para los próximos X meses, el sistema de gestión local de los usuarios utiliza estos derechos para permitir que los receptores « esclavos » accedan a la señal con un mejor granularidad. Esta granularidad se ejerce de acuerdo con dos ejes:

- cada receptor « esclavo » se gestiona de forma individualizada y puede recibir unos derechos propios;
- los derechos concedidos a los receptores « esclavos » están perfectamente controlados y pueden variar cada día.

En el caso de una aplicación de posicionamiento por satélite, un receptor maestro abonado a la infraestructura de servicio adquiere, como tal, no solo la información de posicionamiento difundida por la señal de servicio, sino también los derechos que le permiten prolongar su acceso a la señal de servicio en el tiempo.

El o los receptores esclavos se gestionan en el nivel local de la red de comunicación segura y no de manera centralizada en la infraestructura. Estos son independientes del receptor maestro gestionado de manera centralizada y, como tales, se someten a las mismas restricciones en términos de política de seguridad.

Los receptores esclavos reciben:

- Una clave de base al comienzo de la misión. Esta clave extremadamente sensible se debe almacenar de forma segura en el receptor. Se inyecta en el receptor esclavo en un medio perfectamente seguro y controlado, por ejemplo, utilizando una red segura que permita conectar los receptores « esclavos » con el sistema de gestión local de los usuarios.
- De manera regular, una clave oculta que les permite acceder a la señal de servicio. Estos descifran esta clave utilizando su propia clave de base, a continuación utilizan la clave obtenida de este modo para

demodular la señal de servicio. Esta clave les da como mínimo el acceso a la señal por 24 horas, por ejemplo, al sistema de gestión local de los abonados, utilizando un canal de distribución seguro que permite de este modo controlar los receptores « esclavo » cifrados mediante su propia clave de base. Esto permite utilizar una red de comunicación con una baja protección de privacidad para transmitir los derechos de los usuarios. En los receptores « esclavo » se aplica un procedimiento de reconstrucción de claves que permite el acceso a los servicios seguros distribuidos por la infraestructura a partir de los derechos transmitidos por el sistema de gestión local de los usuarios.

Los receptores « esclavos », por sus reducidas funciones de denegación, solo necesitan un juego de claves de duración limitada, que les permita acceder a la señal de acuerdo con los derechos fijados por el sistema de gestión local.

De manera ventajosa, la gestión local de los receptores garantiza la gestión del conjunto de receptores esclavo, la generación y la asignación de claves a estos receptores esclavos, y la distribución de estas claves a los receptores esclavos.

El algoritmo de cifrado que hay que utilizar para proteger el juego de claves mediante la clave de base se puede seleccionar entre los diferentes algoritmos agregados para proteger las claves.

La seguridad del sistema que se obtiene de este modo es al menos tan importante como la que ofrece un sistema centralizado. En efecto, el sistema de gestión centralizada de los receptores controla el acceso a la señal de cada receptor esclavo con un granularidad de un día (granularidad mínima ofrecida por la infraestructura S). Esta controla también cada receptor de forma totalmente independiente por medio de la noción de clave de base. Al estar dotado cada receptor esclavo de su propia clave de base, este solo puede adquirir los derechos que tiene asignados y en ningún caso los de los demás receptores. Esta seguridad se basa en unos procedimientos de criptografía.

Sin salirse del marco de la invención, el sistema y las etapas que se han descrito con anterioridad, se pueden utilizar en cualquier sistema que integre una capacidad de comunicación, todos los emisores/receptores de radio y terminales que integran una capacidad de comunicación, cualquier solución de red inalámbrica, del tipo red S-Wimax, S-Wifi, UWB, las infraestructuras de los bancos,…

REIVINDICACIONES

1. Sistema que permite gestionar la distribución de claves de acceso a unos servicios ofrecidos por una infraestructura de una manera descentralizada, que comprende una red de comunicación, un dispositivo de emisión de mensajes, en el que los usuarios se agrupan en « grupo de usuarios » que comparten las mismas características y que deben someterse a las mismas restricciones decididas de manera centralizada, comprendiendo dicho sistema al menos los siguientes elementos:

- un receptor maestro (12) y uno o varios receptores esclavos (18);
- un centro de comunicación centralizada (11) que comprende unos medios (13) que permiten la gestión local de receptores esclavos:
- un receptor maestro (12). que comprende un módulo de recepción de los derechos contenidos en la señal emitida por la infraestructura y de extracción de un sistema de claves (15), así como la asignación (17) a los receptores esclavos que forman parte de un mismo grupo de usuarios de todas o una parte de las claves extraídas;
- dicho receptor « maestro » (12) integra todas las funciones de seguridad y actúa como retransmisor inteligente frente a los receptores « esclavos » (18);
- un medio de distribución (21, 22) de las claves extraídas del receptor maestro hacia los receptores esclavos en función de los derechos asociados a dichos receptores esclavos, cifrándose las claves mediante una clave de base asociada a un receptor;
- un receptor esclavo (18), que comprende un medio de extracción (19) de al menos una parte de las claves distribuidas por la infraestructura y un medio (20) adaptado para recibir una o varias claves de autorización de acceso a uno o varios servicios a partir de los derechos transmitidos por el receptor maestro, y comprendiendo dicho receptor esclavo un módulo de memorización de una clave de base.

2. Sistema de acuerdo con la reivindicación 1, **caracterizado porque** los medios de distribución de las claves entre un receptor maestro y un receptor esclavo comprenden una conexión segura y una conexión no segura.

3. Sistema de acuerdo con la reivindicación 1, **caracterizado porque** el sistema es un sistema de posicionamiento por satélite y **porque** los servicios son información de navegación.

4. Procedimiento de gestión descentralizada de un sistema seguro, que comprende una infraestructura que proporciona diferentes servicios a diferentes usuarios, en el que los usuarios están agrupados en « grupo de usuarios » que comparten las mismas características y que deben someterse a las mismas restricciones decididas de manera centralizada y que comprende al menos las siguientes etapas:

- transmitir una señal con un función centralizada, comprendiendo dicha señal información sobre los servicios y los derechos de los usuarios;
- un receptor maestro (12) recibe una señal de la infraestructura así como las claves de autorización de acceso a un servicio para un usuario determinado;
- dicho receptor « maestro » (12) integra todas las funciones de seguridad y actúa como retransmisor inteligente frente a los receptores « esclavos » (18);
- dicho receptor maestro (12) extrae los derechos asociados a un usuario, extrae un sistema de claves, asigna toda o una parte de estas claves a los receptores esclavos (18) y difunde las claves asignadas hacia los receptores esclavos, cifrándose las claves mediante un clave de base asociada a un receptor;
- dichos receptores esclavos descifran la clave que les da acceso a un servicio determinado a partir de su clave de base.

5. Procedimiento de gestión de acuerdo con la reivindicación 4, **caracterizado porque** los servicios son unos servicios de navegación y la transmisión de las señales se realiza vía satélite.

6. Procedimiento de gestión de acuerdo con la reivindicación 4, **caracterizado porque** se utiliza una conexión segura para transmitir la clave de base.

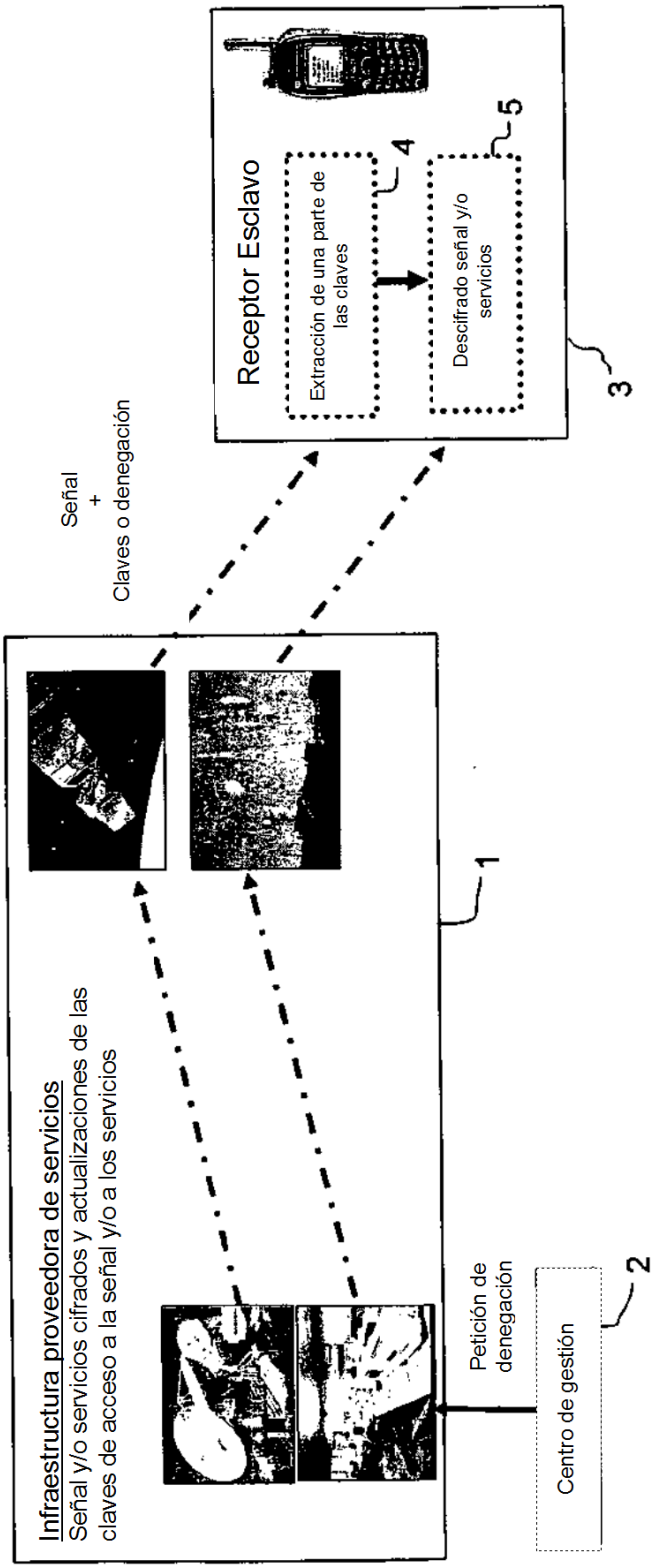
Receptor Esclavo
Extracción de una parte de las claves
Descifrado señal y/o servicios
4
5
3
Señal
+
Claves o denegación
Infraestructura proveedora de servicios
Señal y/o servicios cifrados y actualizaciones de las claves de acceso a la señal y/o a los servicios
1
Petición de denegación
Centro de gestión
2

FIG.1

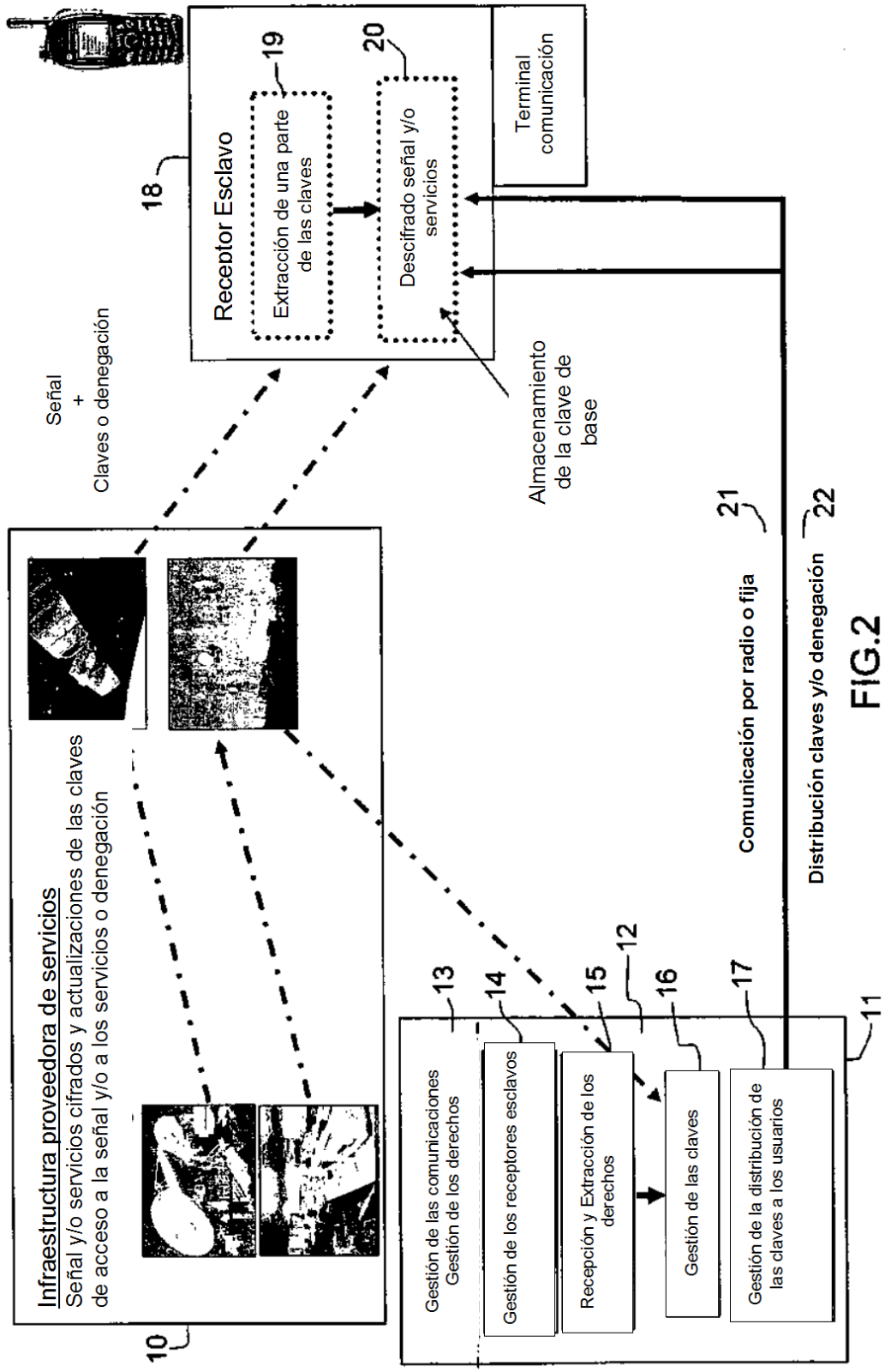
Infraestructura proveedora de servicios
Señal y/o servicios cifrados y actualizaciones de las claves de acceso a la señal y/o a los servicios o denegación
10
Señal + Claves o denegación
Receptor Esclavo
18
Extracción de una parte de las claves
19
Descifrado señal y/o servicios
20
Terminal comunicación
Almacenamiento de la clave de base
Comunicación por radio o fija
21
Distribución claves y/o denegación
22
Gestión de las comunicaciones Gestión de los derechos
13
Gestión de los receptores esclavos
14
Recepción y Extracción de los derechos
15
12
Gestión de las claves
16
Gestión de la distribución de las claves a los usuarios
17
11

FIG.2