

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 584 334**

51 Int. Cl.:

H04W 8/20 (2009.01)

G06F 21/00 (2013.01)

H04L 29/06 (2006.01)

H04W 8/18 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **05.12.2011 E 11793753 (2)**

97 Fecha y número de publicación de la concesión europea: **23.03.2016 EP 2649826**

54 Título: **Método para gestionar el contenido de un elemento seguro conectado a un equipo**

30 Prioridad:

06.12.2010 EP 10306359

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

27.09.2016

73 Titular/es:

**GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR**

72 Inventor/es:

**GIRARD, PIERRE y
PROUST, PHILIPPE**

74 Agente/Representante:

ISERN CUYAS, María Luisa

ES 2 584 334 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Método para gestionar el contenido en un elemento seguro conectado a un equipo.

- 5 La presente invención se refiere a un método para gestionar el contenido en un elemento seguro conectado a un equipo.

10 Un elemento seguro es normalmente una UICC (Tarjeta Universal de Circuito Integrado) incrustada en una aplicación Sim, estando instalado dicho elemento de seguridad, de modo fijo o no, en un terminal, como por ejemplo un teléfono móvil o una máquina (para aplicaciones M2M (Máquina a Máquina)).

15 Una UICC puede tener el formato de una tarjeta inteligente, o puede estar en cualquier otro formato como por ejemplo, pero no limitado a, un chip envasado como el descrito en la PCT/SE2008/050380, o cualquier otro formato. Se puede utilizar, por ejemplo, en terminales móviles en redes GSM y UMTS. La UICC garantiza la autenticación de la red, integridad y seguridad de todo tipo de datos personales.

20 En una red GSM, la UICC contiene principalmente una aplicación SIM y en una red UMTS es la aplicación USIM. Una UICC puede contener varias otras aplicaciones, haciendo posible que la misma tarjeta inteligente pueda dar acceso tanto a la red GSM como a la UMTS, y también proporcionar el almacenamiento de una guía telefónica y otras aplicaciones. También es posible acceder a una red GSM usando una aplicación USIM y es posible acceder a las redes UMTS mediante una aplicación SIM con los terminales móviles preparados para tal fin. Con el UMTS versión 5 y mas tarde con una red escenario como la LTE, se requiere una nueva aplicación, el Módulo de Identidad de Servicios Multimedia IP (ISIM) para los servicios en el IMS (Subsistema Multimedia IP). La guía telefónica es una aplicación independiente y tampoco forma parte de ningún módulo de información de suscripción.

30 En una red COMA, la UICC contiene una aplicación CSIM, además de aplicaciones SIM y 3GPP USIM.

35 Una tarjeta con las tres características se llama una tarjeta de identidad de usuario extraíble, o R-UIM. Por lo tanto, la tarjeta R-UIM se puede insertar en terminales CDMA, GSM o UMTS, y funcionará en los tres casos.

40 En las redes 2G, la tarjeta SIM y la aplicación SIM estaban unidas, por lo que "la tarjeta SIM" podría referirse a la tarjeta física, o cualquier tarjeta física con la aplicación SIM.

La tarjeta inteligente UICC consiste en una CPU, ROM, RAM, EEPROM y circuitos I/O. Las primeras versiones consistían en tarjetas inteligentes de tamaño completo (85 x 54 mm. ISO/IEC 7810 ID-1).

45 Dado que la ranura de la tarjeta ha sido estandarizada, un abonado puede mover fácilmente su cuenta inalámbrica y su número de teléfono de un terminal a otro. Esto también transferirá su agenda telefónica y sus mensajes de texto. De similar modo, por lo general un abonado puede cambiar de operador mediante la inserción de la tarjeta UICC de un nuevo operador en su terminal. Sin embargo, esto no siempre es posible debido a que algunos operadores (por ejemplo, en los Estados Unidos) bloquean el cambio de SIM

50

en los teléfonos que ellos venden, evitando que se puedan utilizar en ellos las tarjetas de los operadores de la competencia.

5 La integración del marco ETSI y del marco de gestión de aplicaciones de la Plataforma Global se ha estandarizado en la configuración de la UICC.

Las UICCs están estandarizadas por 3GPP y ETSI.

10 Una UICC normalmente se puede extraer de un terminal móvil, por ejemplo cuando el usuario desea cambiar su terminal móvil. Después de haber insertado su UICC en su nuevo terminal, el usuario mantendrá aún el acceso a sus aplicaciones, contactos y credenciales (operador de red).

15 También es conocido el hecho de soldar o fijar la UICC a un terminal, con el fin de conseguir que sea dependiente del terminal. Esto se hace en aplicaciones M2M (Máquina a Máquina). Se alcanza el mismo objetivo cuando un chip (un elemento seguro) que contiene las aplicaciones y archivos SIM o USIM está contenido en el terminal. El chip es, por ejemplo soldado a la placa madre del terminal o máquina y constituye una UICC.

20 Algunas de las soluciones conocidas se aplican a estas e-UICCs soldadas o a estos chips que contienen las mismas aplicaciones que los chips comprendidos en las UICCs. Se puede realizar una copia de las UICCs que no están totalmente vinculadas a dispositivos, pero que son extraíbles con dificultad porque no están pensadas para ser extraídas, situadas en terminales distantes o profundamente integradas en máquinas. Un factor de forma especial de la UICC (muy pequeña, por ejemplo, y por lo tanto difíciles de manejar) también puede ser una razón para considerarla de facto integrada en un terminal. Lo mismo se aplica cuando una UICC está integrada en una máquina que no está destinada a ser abierta.

30 En la siguiente descripción, las UICCs soldadas o los chips que contienen o están diseñados para contener las mismas aplicaciones que las UICCs se denominarán generalmente UICCs incrustadas o elementos de seguridad incrustados (en contraste con las UICCs extraíbles o elementos de seguridad extraíbles). Esto también se aplicará a las UICCs o los elementos de seguridad que son extraíbles con dificultad.

35 La invención hace referencia a la gestión remota de un elemento seguro como una UICC localizada en o dentro de un dispositivo que puede ser infectado por software contaminado. Esta invención se aplica a UICCs incrustadas (e-UICCs) y a UICCs extraíbles. El término "elemento seguro" se utilizará de manera general en la siguiente descripción para designar a estas UICCs.

40 Se conoce que, una vez entregado, el elemento seguro necesita ser mantenido durante toda su vida útil. El mantenimiento usualmente consiste en actualizaciones remotas del contenido del elemento seguro. Esta podría ser una personalización avanzada, un código parche, una instalación de una nueva funcionalidad, una actualización de datos, la renovación de una clave, etc. Estas operaciones son realizadas por una plataforma de administración remota que opera a través de una red potencialmente insegura (por ejemplo, internet) y un dispositivo potencialmente inseguro al cual se conecta el elemento de seguridad.

50

La Figura 1 representa un sistema en el que un elemento seguro incluido en un terminal 21 descargar contenidos de una plataforma administrativa 22 a través de internet 23. El software contaminado 24 puede estar presente a nivel de internet 23 o el software contaminado 25 a nivel del terminal 21.

5

A fin de asegurar el proceso, existe un protocolo de comunicación seguro extremo-a-extremo entre la plataforma de administración y el elemento seguro (por ej. un protocolo de Plataforma Global). Sin embargo, en la mayoría de los casos, ni el servidor ni el elemento seguro disponen de una conectividad directa el uno con el otro y hay algún "middleware" en el dispositivo que inicia la sesión de administración segura. Se conoce que la primera sesión entre el middleware y el servidor ha de ser también segura (por ej. con TLS) por múltiples razones (petición de autenticación de gestión remota, confidencialidad de la petición, evitar denegación de servicio, etc.).

10

15 Sin embargo, si se localiza algún software contaminado en el terminal, este puede ser utilizado por un hacker para realizar algún tipo de manipulación remota en el elemento seguro por cuenta del dispositivo de la víctima en el que el software contaminado se ha instalado, tal como se muestra en la figura 2.

20 En esta figura, el software contaminado 25 esta situado en el terminal de la víctima 21. Incluso si el canal entre el terminal 21 y la plataforma de administración 22 está asegurado mediante TLS, el software contaminado 25 puede dirigir el contenido (datos y software) a otro elemento seguro 26 localizado en el terminal del hacker 27 a través de internet 23. Esta redirección del contenido descargado puede ser muy lesiva para el propietario del terminal 21. Por ejemplo, en el dominio Telecom, se puede prever descargar una aplicación SIM completa en un elemento seguro ya existente 20. Para ello, el usuario del terminal 21 conecta con la plataforma administradora 22 a través de internet y solicita una suscripción a un MNO dado (la plataforma de administración puede ser conectada a diferentes MNOs como se vera mas adelante). La plataforma 22 reconoce el terminal del usuario 21 y tras su identificación, prepara el contenido a descargar (aplicación Sim, datos, credenciales entre ellos IMSI y Ki). Si el contenido es descargado en el elemento seguro 26 del hacker en lugar de en el elemento seguro 20, el propietario del terminal 21 no podrá conectar, no sólo a su red MNO, sino que pagará las comunicaciones del hacker.

25

35 Además, la credencial utilizada para autenticar el dispositivo puede ser robada por el software contaminado.

40 Utilizar el elemento seguro como tal para autenticar el dispositivo también resulta dificultoso por dos razones. Primero, el elemento seguro se encuentra bajo gestión, por lo que es difícil utilizarlo (especialmente si no esta personalizado o si la personalización no esta finalizada). Y segundo, la credencial que contiene poder pertenecer a otra entidad que poder no ser la que opera la plataforma de gestión remota.

45 El documento US 2008/261561 revela un método para transferir credenciales Sim "soft" desde un dispositivo móvil emisor a un dispositivo móvil objetivo a través de un servidor de red. Se establece una conexión segura entre el dispositivo móvil emisor y el servidor antes de la transferencia de las credenciales al servidor. Las credenciales son entonces borradas en el dispositivo móvil emisor y se instalan en un dispositivo móvil objetivo.

50

5 El documento WO 2009/103623 revela un sistema para asociar un dispositivo inalámbrico 'genérico', es decir, un dispositivo que no está pre-programado con credenciales de suscripción (USIM) correspondiente a un operador particular, con un Operador de Origen designado por el propietario del dispositivo. El sistema facilita el enlace automático de un dispositivo recientemente activado M2M con un servidor apropiado a fin de descargar las credenciales de suscripción para el Operador de Origen.

10 El documento 3GPP TR 33.812 v1.0.0 de Septiembre de 2008 concierne a la gestión remota de manera segura de una aplicación USIM/ISIM en un equipo M2M.

10 El documento 3GPP2, C.S0040, versión 1.0, 18 Julio 2003 (2003-07-18), "IP Based Over-the-Air Handset Configuration Management (IOTA-HCM)" se refiere a la actualización de parámetros COMA almacenados en estaciones móviles.

15 Ninguno de estos documentos propone verificar, al nivel de un servidor o una plataforma de administración, que una petición para gestionar un elemento seguro proviene del mismo elemento seguro que ha establecido con esta plataforma un canal seguro con claves de sesión. Es por ello posible para un hacker instalar software malicioso en el equipo que actúa en el contenido gestionado por la plataforma, con objeto de
20 redireccionar los datos a otro elemento seguro.

La presente invención propone una solución a esos problemas.

25 A este respecto, la presente invención concierne a un método para gestionar contenido en un elemento seguro conectado a un equipo, siendo el contenido gestionado en el elemento seguro desde una plataforma administradora distante, consistiendo dicho método en:

- 30 - Establecer, al nivel de la plataforma de administración, un canal seguro entre el equipo y la plataforma de administración, gracias a claves de sesión generadas por el elemento seguro y transmitidas al equipo:
- Transmitir, a la plataforma de administración, una petición para gestionar el contenido del elemento seguro;
- 35 - Verificar, al nivel de la plataforma de administración, que la petición proviene del mismo elemento seguro que ha generado las claves de sesión y, si resulta positiva, autorizar la gestión y, si resulta negativa, prohibir la gestión.

40 La gestión antes mencionada consiste en al menos una de las siguientes tareas:

- Descargar contenido en el elemento seguro
- Eliminar contenido en el elemento seguro
- 45 - Exportar contenido almacenado en el elemento seguro
- Activar contenido almacenado en el elemento seguro
- 50 - Desactivar contenido almacenado en el elemento seguro

La verificación puede consistir en comprobar que la clave privada utilizada para establecer el canal seguro corresponde a un certificado suministrado al elemento seguro sobre el cual se ha solicitado la gestión.

5 En otra realización, la verificación consiste en comprobar que un identificador correspondiente a una clave simétrica utilizada para establecer el canal seguro corresponde a un identificador del elemento seguro sobre el cual se ha solicitado la gestión.

10 La presente invención se entenderá mejor al leer la siguiente descripción de las figuras 3 y 4, donde:

- La Figura 3 representa una primera etapa del método de la presente invención;

15 - La Figura 4 representa una segunda etapa del método de la presente invención:

La invención propone insertar en el elemento seguro una aplicación independiente que se usará para asegurar la sesión entre la plataforma de administración y el terminal. Después de este paso, el servidor verifica la conexión entre la identidad a nivel de sesión del dispositivo y la identidad en la gestión remota del elemento seguro.

20

La Figura 3 representa una primera etapa del método de la presente invención.

Como se puede observar, el elemento seguro 20 incluye una aplicación 28 prevista para proporcionar claves de sesión a la plataforma de administración 22. Estas claves de sesión son generadas por la aplicación 28 y transmitidas al equipo 21. La aplicación 28 transmite también un identificador o un certificado al equipo 21.

25

- Se envía un identificador desde la aplicación 28 al equipo cuando se usa una encriptación simétrica (sobre la base de claves secretas) para crear un canal seguro entre la plataforma 22 y el equipo 21. El equipo 21 transmite este identificador a la plataforma 22. La plataforma 22 compara entonces el identificador recibido con los identificadores que almacena, a fin de reconocer qué aplicación envió el identificador. Una vez reconocido, la plataforma 22 asocia una clave simétrica al identificador de la aplicación 28. La aplicación 28 y la plataforma 22 obtienen entonces claves de sesión para encriptar (por razones de confidencialidad) y mantener la integridad de la comunicación entre el equipo 21 y la plataforma 22. Se ha establecido así un canal seguro entre el equipo 21 y la plataforma 22 (ejemplos de estos protocolos están estandarizados por Plataforma Global, también se puede utilizar PSK-TLS).

30

35

40

- Otra manera de crear este canal seguro consiste en intercambiar certificados entre la plataforma 22 y la aplicación 28. La plataforma autentica la aplicación 28 solicitándole que firme un "hash" de todos los mensajes ya intercambiados. El equipo 21 genera una clave de sesión y la encripta para la plataforma 22. Se establece entonces una comunicación segura (un ejemplo de esta estandarizada es TLS) entre el equipo 21 y la plataforma 22.

45

En ambos casos precedentes, se ha establecido un canal seguro entre la plataforma y el equipo 21.

La segunda etapa principal de la invención consiste en verificar la conexión entre la identidad a nivel de sesión del dispositivo y la identidad en la gestión remota del elemento seguro.

5 La Figura 4 representa esta etapa.

Se envía una petición de gestión del contenido del elemento seguro a la plataforma de administración. Esta gestión consiste, por ejemplo, en descargar contenido en el elemento seguro 20, eliminar o exportar contenido almacenado en el 6 activar o
10 desactivar contenido almacenado en él. La descarga de contenido puede consistir, por ejemplo, en descargar una aplicación Sim completa en el elemento seguro, con las credenciales asociadas (IMSI, Ki). También puede consistir en descargar una guía de teléfonos desde la plataforma 22 en el elemento seguro 20.

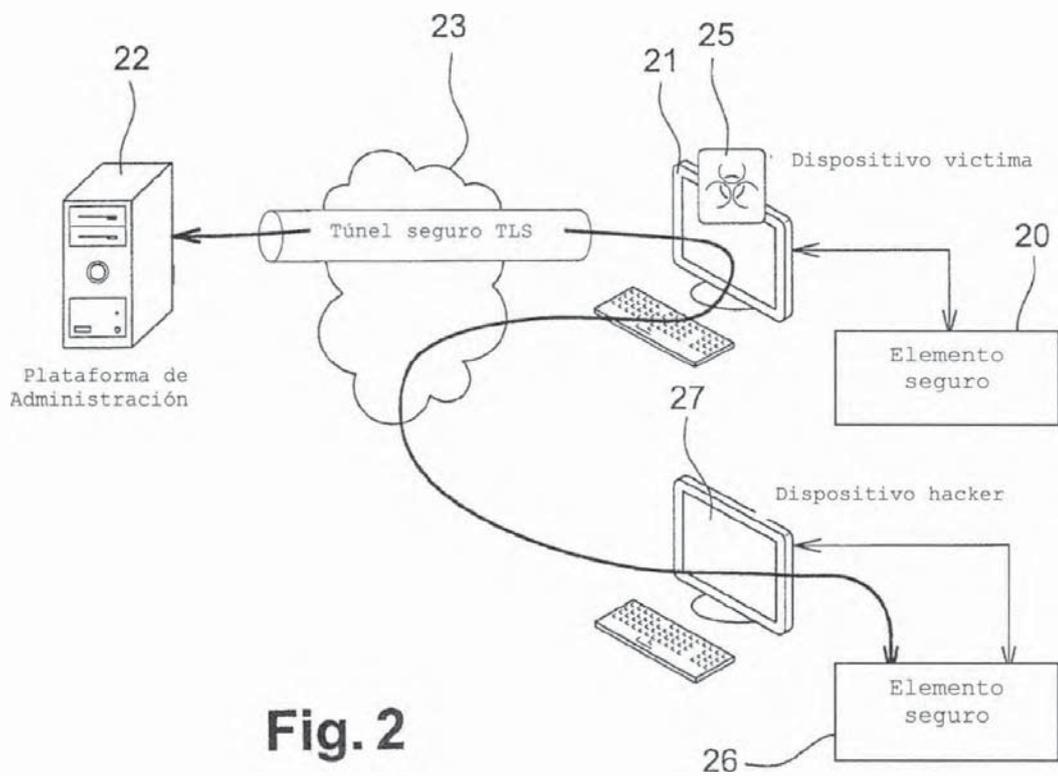
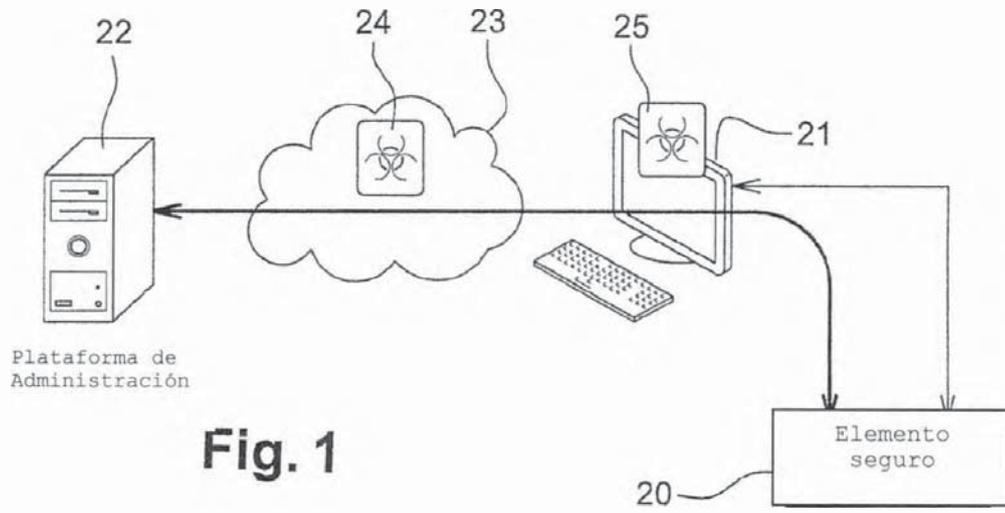
15 A fin de verificar esta conexión, el elemento seguro 20 envía a través del canal seguro establecido, un identificador fijado, como por ejemplo su ICCID o su número de serie. La plataforma 22 comprueba que esta petición proviene del mismo elemento seguro (por ejemplo las claves de sesión utilizadas para establecer el canal seguro se comparan con el identificador fijado). Si la comprobación es positiva, la gestión es autorizada. De lo
20 contrario, sí la comprobación es negativa, se prohíbe la gestión.

La invención asegura que el elemento seguro que es gestionado es el correcto y que no se trata de otro elemento seguro conectado a la plataforma mediante software contaminado.

25 El equipo 21 puede ser móvil o fijo, por ejemplo compuesto por una máquina.

REIVINDICACIONES

- 5 1. Método para gestionar contenido en un elemento seguro (20) conectado a un equipo (21), dicho contenido estando gestionado en dicho elemento seguro (20) desde una plataforma de administración remota (22), en el que dicho método consiste en:
- Establecer, al nivel de dicha plataforma de administración (22), un canal seguro entre dicho equipo (21) y dicha plataforma de administración (22),
10 y estando **caracterizado** porque dicho canal seguro se establece gracias a claves de sesión generadas por dicho elemento seguro (20) y transmitidas a dicho equipo (21);
 - 15 - Transmitir, a dicha plataforma de administración (22), una petición para gestionar el contenido de dicho elemento seguro (20);
 - 20 - Verificar, al nivel de dicha plataforma de administración (22), que dicha petición proviene del mismo elemento seguro (20) que ha generado dichas claves de sesión y, si resulta positiva, autorizar dicha gestión y, si resulta negativa, prohibir dicha gestión.
- 25 2. Método de acuerdo con la reivindicación 1, en el que dicha gestión consiste en al menos una de las siguientes tareas:
- Descargar contenido en dicho elemento seguro (20)
 - Eliminar contenido en dicho elemento seguro (20)
 - 30 - Exportar contenido almacenado en dicho elemento seguro (20)
 - Activar contenido almacenado en dicho elemento seguro (20)
 - Desactivar contenido almacenado en dicho elemento seguro (20).
- 35 3. Método de acuerdo con las reivindicaciones 1 o 2, en el que dicha verificación consiste en comprobar que la clave privada utilizada para establecer dicho canal seguro corresponde a un certificado suministrado al elemento seguro (20) sobre el que se ha solicitado la gestión.
- 40 4. Método de acuerdo con las reivindicaciones 1 o 2, en el que dicha verificación consiste en comprobar que un identificador correspondiente a una clave simétrica utilizada para establecer dicho canal seguro corresponde a un identificador del elemento seguro (20) sobre el que se ha solicitado la gestión.
- 45 5. Método de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que dicho equipo (21) se trata de un equipo móvil.
- 50 6. Método de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que dicho equipo (21) se trata de un equipo fijo.



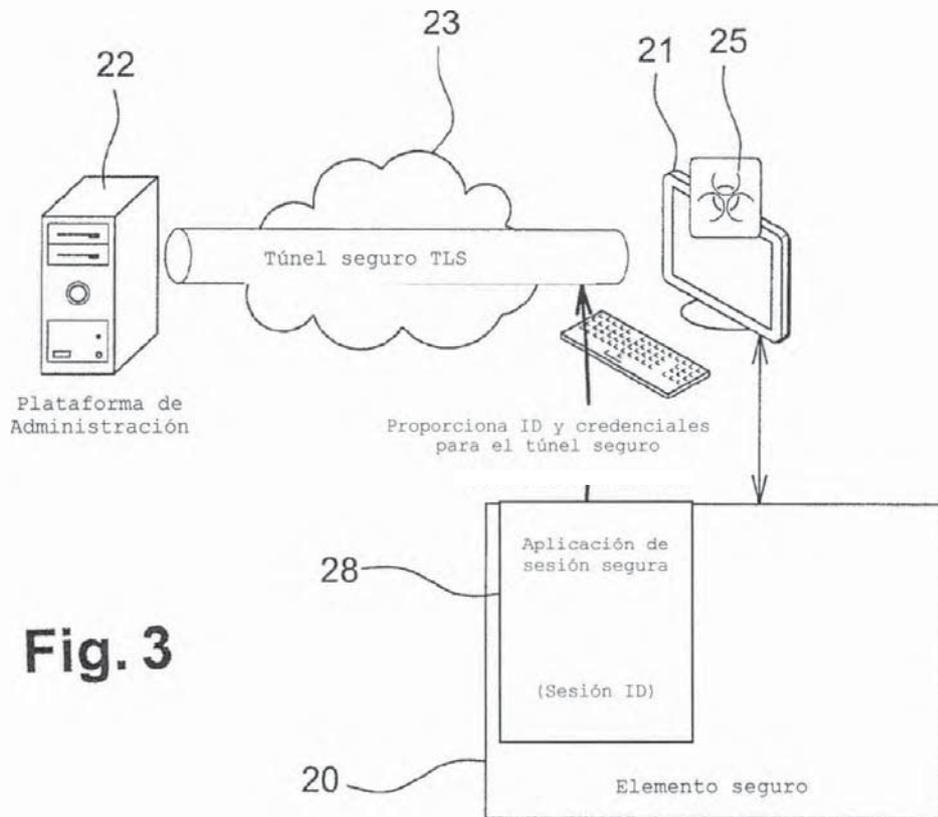


Fig. 3

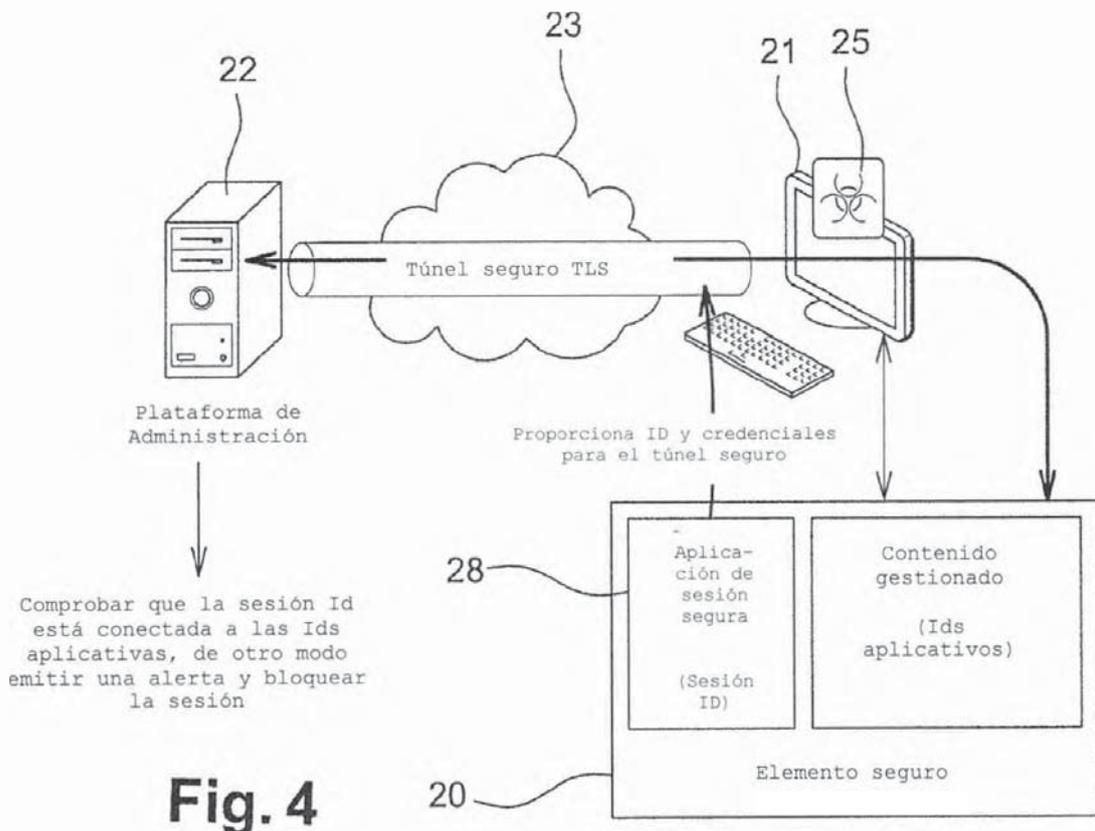


Fig. 4