(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 385 910**

(51) Int. CI.:
G06F 21/00 (2006.01)
G06F 21/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07251512 .5**
(96) Fecha de presentación: **05.04.2007**
(97) Número de publicación de la solicitud: **1843273**
(97) Fecha de publicación de la solicitud: **10.10.2007**

(54) Título: **Módulo seguro para proporcionar valores horarios de confianza**

(30) Prioridad:
06.04.2006 GB 0606962

(45) Fecha de publicación de la mención BOPI:
03.08.2012

(45) Fecha de la publicación del folleto de la patente:
03.08.2012

(73) Titular/es:
VODAFONE GROUP PLC
VODAFONE HOUSE THE CONNECTION
NEWBURY
BERKSHIRE RG14 2FN, GB

(72) Inventor/es:
Montaner, Javier;
Koraichi, Najib y
Moutarazak, Said

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Módulo seguro para proporcionar valores horarios de confianza

La presente invención se refiere a un módulo seguro para proporcionar un reloj de confianza. En particular, la invención se refiere al suministro de un módulo tal, para incorporarlo dentro de un dispositivo portátil en red.

En el campo de los servicios de telecomunicaciones móviles, es posible que algunos servicios requieran la utilización de valores de fecha/hora para ejecutarse: un ejemplo podría ser un servicio de entrega de contenido "embargado", que permita reproducir un elemento de contenido solamente antes o después de una fecha determinada. Si estos servicios han de suministrarse sin conexión (es decir, no es posible acceder a un reloj en red), el proveedor de los servicios debe recurrir a un reloj local. No obstante, este origen de la hora puede no ser exacto. Además, es posible que los usuarios sin escrúpulos intenten modificar el valor de la hora local almacenado en un reloj local, para evadir las limitaciones temporales impuestas por los servicios.

La ejecución dependiente del tiempo de los servicios de entrega de contenido puede mediarse utilizando técnicas de gestión de derechos digitales (DRM). Es posible imponer límites de tiempo a la descarga y a la reproducción de elementos de contenido utilizando técnicas básicas de la DRM.

Los protocolos como el OCSP (protocolo del estado de los certificados con conexión a red) proporcionan un modo para validar la confiabilidad de los certificados en tiempo real/con conexión. Las respuestas del OCSP incluyen una marca de hora que indica el momento en que se generó la respuesta. En las normas de la OMA (Open Mobile Alliance) relativas a la DRM, este valor se utiliza para sincronizar/renovar la hora DRM de los dispositivos que se han desincronizado. Este método para obtener una hora segura requiere una conexión en tiempo real con el servidor OCSP.

En la solicitud de patente británica n.º de publicación GB2403382, el solicitante describe un sistema de entrega DRM que facilita la entrega de contenido limitada en el tiempo, recurriendo a la presencia de un reloj que es exacto y resistente a modificaciones no autorizadas. Uno de esos relojes, que en la solicitud del solicitante se denomina reloj de referencia principal (PRC), funciona sobre la base de señales de sincronización recibidas de un sistema de posicionamiento global (GPS).

Se sabe que esto proporciona lo que se denomina un "reloj seguro" en los dispositivos electrónicos. Un ejemplo particular de este tipo de "reloj seguro" que utiliza una tarjeta inteligente incorporada a un dispositivo de comunicaciones móviles se describe en la solicitud de patente internacional WO2004/075525.

Como se muestra en la WO2004/075525, es posible adaptar un módulo seguro para que funcione como origen de hora de confianza sin conexión en los dispositivos portátiles en red. Aquí, una vez que el módulo de identificación del abonado (SIM) recibe un valor horario de un servidor horario remoto, dicho valor se utiliza como referencia a la que se añade un tiempo inferido desde un contador de tiempo asociado al SIM. En este caso, para incrementar el contador de tiempo, el módulo seguro depende de una fuente externa (el reloj del dispositivo), que es básicamente menos confiable que el módulo seguro en sí mismo.

Otros documentos conocidos son la EP1022640, en la que se describe un dispositivo marcador de la hora de confianza que deja de funcionar luego de que se cumplen determinadas condiciones, y la WO2004/102967, en la que se describe un método que permite determinar la fecha y hora de vencimiento para acceder a datos cifrados, en un módulo seguro que utiliza un reloj interno para proporcionar la hora actual.

En particular, en la EP1022640 se describe un dispositivo marcador de la hora de confianza que se puede conectar a un ordenador por medio de una conexión SCS1, a fin de proporcionar a ese ordenador una marca de hora de confianza, que es necesaria para que se siga ejecutando el software en el ordenador. Este dispositivo marcador de la hora de confianza se inhabilita luego de haber emitido una cantidad preestablecida de marcas de hora, o luego de transcurrido un tiempo de uso determinado. Asimismo, este dispositivo marcador de la hora de confianza controla el desfase de su reloj interno por medio de una referencia horaria externa, mientras mantiene marcas de hora que se incrementan de forma monótona.

Por consiguiente, un objeto de la invención es evitar o por lo menos mitigar los problemas antemencionados.

De acuerdo con un aspecto de la presente invención, se proporciona un método conforme con la reivindicación independiente 1 y un sistema conforme con la reivindicación independiente 2.

Convenientemente, el método comprende asimismo restablecer a un valor predeterminado el conteo de la cantidad de veces en las que se utiliza el valor horario almacenado, a consecuencia de lo cual se desbloquea el suministro de servicios limitados en el tiempo de acuerdo con el valor horario almacenado.

Este contador de transacciones brinda flexibilidad, y al mismo tiempo mantiene el control en manos del proveedor de la red. Además, se elimina la participación del usuario, al utilizar el contador de transacciones para limitar el uso de la función de hora segura y obligar a que se solicite al servidor un nuevo valor horario para desbloquear la función limitada.

Los eventos de actualización pueden ocurrir a intervalos predeterminados. Si lo hacen, los intervalos predeterminados pueden ser de duración variable, y la duración variará de acuerdo con la frecuencia de servicio necesaria.

Es preferible que el valor horario actualizado se entregue en un formato cifrado.

El evento de actualización puede ser el resultado de un mensaje de difusión emitido por la red de comunicaciones.

Mediante la utilización de técnicas de difusión y/o de envío (*push*) para distribuir el valor horario a todos los SIM, el método garantiza que el dispositivo se actualice sin la participación del usuario. La solución que funciona sobre la base de la difusión es conveniente para los servicios de entrega de difusión (p. ej. DVB-H) y facilita el acceso universal para todos los dispositivos (protegidos), no solo los dispositivos móviles. Dado que este método no depende de la información recibida de otros dispositivos, sino solo del servidor, la seguridad es mayor.

La red de comunicaciones puede ser una red de comunicaciones alámbrica o inalámbrica.

El método puede comprender asimismo, mientras el dispositivo de comunicación permanece desconectado de la red, llevar un registro de las veces que el valor horario almacenado se utiliza para determinar el acceso al servicio limitado en el tiempo; y, cuando el dispositivo de comunicación se conecta a la red, transmitir el registro a un servidor de registro, lo que permite consolidar el uso del servicio limitado en el tiempo.

El servicio limitado en el tiempo puede ser el acceso a contenido protegido por DRM, donde el acceso a la DRM está limitado por condiciones temporales, de modo tal que el método facilita la validación sin conexión a red de los derechos de acceso.

En particular, el método permite controlar por completo las limitaciones temporales de la DRM, sin depender del reloj convencional (no seguro) de un dispositivo. El valor horario obtenido a través de la invención también se puede utilizar para la validación sin conexión a red de certificados. Otros servicios sin conexión se pueden brindar y controlar utilizando el método de la invención.

Asimismo, el manejo del tiempo en el SIM es "inteligente" y no depende de ningún reloj o dispositivo externo que no es de confianza.

Para comprender mejor la presente invención, a continuación se hará referencia, exclusivamente a modo de ejemplo, a los dibujos adjuntos, en los cuales:

la fig. 1 muestra los componentes de un sistema horario seguro que incluye un módulo seguro; y

la fig. 2 ilustra el funcionamiento del módulo seguro de acuerdo con la presente invención.

En el campo de las telecomunicaciones móviles, el módulo de identificación del abonado (SIM) es un ejemplo práctico de dicho módulo seguro. En la explicación que sigue, la invención se ilustra en términos de este campo de las telecomunicaciones móviles y, por consiguiente, el módulo seguro se denomina SIM en todo el texto. Como los especialistas comprenderán fácilmente, no se pretende limitar la invención al uso de un SIM.

El sistema horario seguro 100 de la fig. 1 incluye un servidor de registro 102, un servidor horario 104, un solicitante de servicio sin conexión a red 106 y un SIM 108.

Mientras el SIM se encuentra en línea (conectado a una red de telecomunicaciones móviles), es posible establecer una conexión con el servidor horario 104, mediante lo cual se puede proporcionar al SIM 108 un valor horario actual seguro 112. De modo opcional, la entrega del valor horario actual seguro 112 podría activarse mediante la recepción de una solicitud 110 enviada desde el SIM 108.

El SIM 108 se puede usar para almacenar una copia local de un valor horario seguro y verificar si el valor horario actual seguro proporcionado por el servidor horario 104 es más reciente que la copia local de un valor horario seguro, para solo actualizar el valor horario local cuando el valor horario actual sea más reciente. En las redes GSM y UMTS/3G, el SIM 108 por lo general se conecta a la red a intervalos breves y regulares (del orden de los minutos). Por consiguiente, la copia local de un valor horario seguro se actualiza con frecuencia.

El SIM 108 está dispuesto para controlar los eventos de solicitud de valor horario. De este modo, el SIM 108 puede inferir cuánto tiempo ha transcurrido desde que se recibió el último valor horario actualizado del servidor horario 104

y/o detectar posibles usos indebidos. Controlar los eventos de solicitud permite realizar una gestión inteligente de la hora en el SIM 108, con lo que se minimiza la dependencia de relojes o dispositivos externos que no son de confianza. De este modo, el SIM opera como un contador de transacciones, con lo que limita el uso (indebido) del valor horario almacenado localmente y, de ser necesario, obliga a solicitar un nuevo valor horario 112 al servidor horario 104.

Con frecuencia, los dispositivos o los servicios que se ejecutan en los dispositivos requieren un valor horario cuando el SIM 108 se encuentra provisoriamente desconectado de la red. En la fig.1, el dispositivo/servicio aparece indicado en términos generales como solicitante de servicio sin conexión a red106. El solicitante 106 envía un mensaje de solicitud 116, en el que pide un valor horario seguro. En respuesta, se suministra el valor horario local al solicitante 106.

De modo conveniente, el SIM 108 está dispuesto para llevar un registro 120 de dichos mensajes de solicitud de hora 106, de modo tal que la próxima vez que el SIM 108 se vuelva a conectar a la red, el registro 120 puede cargarse al servidor de registro 102.

En una realización preferida de la invención (véase la fig. 2), el SIM almacena un valor horario 214 localmente, y recibe de manera periódica un valor horario actualizado 212, mientras se encuentra conectado a la red. Cuando el valor horario actualizado 212 es más reciente que el valor horario almacenado localmente 214, el valor horario actualizado 212 se almacena de modo seguro (en el SIM 108), para ser usado más adelante. Según cuáles sean las circunstancias, este valor se envía a un destinatario por medio de una comunicación punto a punto (p. ej. como mensaje de un servicio de mensajes cortos, SMS: "un texto"), o por medio de difusión/multidifusión (p.ej. difusión de célula, MBMS, DVB).

El valor horario se puede recibir a través de redes alámbricas y/o inalámbricas, siempre y cuando el SIM se encuentre en última instancia conectado al origen de los valores horarios actualizados de la red (el servidor horario 104). El SIM puede estar conectado, solamente por medio de conexiones alámbricas, al origen de la red, a través de un lector de tarjetas inteligentes. De manera alternativa, el SIM puede estar integrado dentro de un PDA compatible con Wi-Fi, y se puede conectar al origen de la red utilizando una combinación de conexión inalámbrica a un concentrador ADSL inalámbrico y conexión ADSL alámbrica desde ese concentrador.

De forma conveniente, el valor horario actualizado 212 estará protegido mediante criptografía durante la transmisión. Naturalmente, el valor horario almacenado de forma local se puede actualizar con la frecuencia necesaria dada la granularidad temporal de los servicios: según cuáles sean las necesidades, ¡la frecuencia de actualización puede ser del orden de los minutos, las horas, los días o las semanas!

Cuando un servicio que se está suministrando en modo sin conexión a red requiere que se verifique el valor horario, se utiliza el último valor horario actualizado almacenado en el SIM.

Como se puede ver en la fig. 1, el método de la invención garantiza que, por lo menos en el modo sin conexión, se utilice la última hora válida de la red. El SIM está dispuesto para rechazar cualquier valor horario de la red 212 (incluso si este se encuentra firmado, protegido o cifrado), si ese valor es anterior al valor horario 214 almacenado localmente en el SIM.

El método de la invención garantiza asimismo que el valor horario siempre se incremente de forma positiva, es decir, en los dispositivos nunca se podrá restablecer la hora para registrar un valor anterior.

Al usuario sin escrúpulos se le puede ocurrir la idea de intentar evadir esta protección manteniendo el SIM 108 constantemente en modo sin conexión, para aprovechar un valor horario anterior. La invención responde a dichas actividades disponiendo que el SIM lleve un contador de transacciones 218 que controla la cantidad de veces que un valor horario dado almacenado localmente 214 se utiliza sin conexión. Si el contador 218 alcanza determinada cantidad límite, el SIM puede bloquear la función de sincronización hasta recibir un valor horario actualizado apropiado 212 de la red. De modo conveniente, el SIM 108 está dispuesto para activar el envío de una solicitud 210 al reloj de la red la próxima vez que se conecte a ella, lo que permite desbloquear el SIM 108 de forma legítima, cuando la función de sincronización del SIM se haya bloqueado por exceder el límite. De este modo, la invención garantiza que el valor horario 214 almacenado en el SIM 108 esté actualizado. Esta solicitud realizada al servidor horario 104 por parte del SIM 108 puede estar firmada por el SIM 108 y llevar un identificador exclusivo que se incluya en la respuesta del servidor. De este modo, el SIM 108 sabrá que un valor horario 212 recibido del servidor horario 104 corresponde a una activación (a la última) 210 iniciada por el SIM. Cuando se encuentra conectado a la red, el SIM 108 también puede enviar al servidor horario 104 o a otro servidor preconfigurado 102 un registro 220 con todas las solicitudes de valor horario de confianza 214 que recibió mientras se encontraba desconectado. El servidor 104,102 puede entonces tomar medidas sobre la base de las transacciones que se hayan llevado a cabo sin conexión.

En otros modos de realización de la invención, se utilizan otros mecanismos dispuestos en los SIM convencionales, así como en otros módulos seguros. Se pueden adoptar disposiciones alternativas en lo que respecta al reloj, por ejemplo, un reloj externo de entrada y salida, o un reloj interno. Estos mecanismos de reloj más sofisticados se pueden incluso utilizar junto con la hora almacenada de la red, para obtener una hora más exacta sin conexión. En cualquier caso, el valor horario actualizado nunca será menor que el último valor de la red almacenado en el SIM.

Existe la posibilidad de que la seguridad del servidor horario 104 llegue a encontrarse en riesgo. Es posible que el SIM 108 no sea capaz de detectar dicho riesgo, cuando los valores horarios se descargan al SIM mediante un mecanismo de solicitud al servidor (*pull*). Por consiguiente, en otro aspecto de la invención, esta posible desventaja se soluciona añadiendo otra capa de seguridad.

En este aspecto de la invención, se implementa otro contador en el SIM (un "contador de solicitudes"), para controlar la cantidad de veces que se han recibido actualizaciones como valores horarios solicitados al servidor. Si este contador alcanza determinado límite, el SIM inicia un mecanismo de envío (*push*) con seguridad adicional (p. ej. validación de certificados, OCSP, etc.), para obtener el valor horario del servidor.

Puede ser conveniente proporcionar más capacidad funcional cuando el servidor horario 104 no esté disponible.

Como se señaló en la explicación de la técnica previa que figura anteriormente, el SIM se puede disponer para que utilice un reloj local (como por ejemplo el que viene en el auricular). Este valor no es completamente de confianza, pero aun así se puede utilizar en determinadas situaciones, para complementar el método de la invención.

De este modo, por ejemplo, en un modo de realización de la invención, el SIM 108 recibe la hora segura proveniente de la red (TN0), y la almacena. Prácticamente en el mismo momento, el SIM 108 obtiene el valor horario actual de un origen local (TL0) (p. ej. el auricular).

Cuando el SIM necesita un valor horario actual (CT) actualizado, intenta obtener ese valor de la red.

No obstante, cuando el servidor horario 104 (o la red) no se encuentran disponibles, no habrá ningún valor horario (TN1) disponible. Por consiguiente, el SIM 108 calcula el CT de modo local, obteniendo el valor horario actual del origen local TL1.

Luego, el SIM comprueba que el TL1 sea mayor que el TL0, y hace el siguiente cálculo CT = TN0 + (TL1 - TL0). Si TL1 < TL0, entonces CT = TN0. El valor CT no es totalmente de confianza, pero para determinadas situaciones de uso puede ser útil de todos modos, si al usuario no le interesa modificar el valor horario.

REIVINDICACIONES

1. Un método para proporcionar valores horarios de confianza en dispositivos de comunicaciones que cuentan con un medio de almacenamiento seguro (108) y que se pueden emplear para conectarse a una red de comunicaciones (102,104), método que comprende:

almacenar un valor horario (214) en el medio de almacenamiento seguro (108), valor horario que es necesario para determinar el acceso a un servicio limitado en el tiempo;

mientras el dispositivo de comunicaciones se encuentra desconectado de la red de comunicaciones (102,104), contar la cantidad de veces que el valor horario almacenado (214) se utiliza para determinar el acceso al servicio limitado en el tiempo;

solo suministrar servicios limitados en el tiempo de acuerdo con el valor horario almacenado (214), si la cantidad de veces que se ha utilizado el valor horario almacenado no excede un límite de uso predefinido (218);

mientras el dispositivo de comunicaciones móviles se encuentra conectado a la red de comunicaciones (102,104), recibir un valor horario actualizado (212) en un evento de actualización, evento de actualización que es resultado de un mensaje de solicitud (*pull*) (210) emitido por el dispositivo de comunicaciones;

al recibir el valor horario actualizado (212), comparar el valor horario actualizado (212) con el valor horario almacenado (214) en el medio de almacenamiento seguro (108);

solo si el valor horario actualizado (212) es más reciente que el valor horario almacenado (214), almacenar el valor horario actualizado en lugar del valor horario almacenado;

contar la cantidad de veces que el valor horario almacenado (214) se actualiza con un valor horario solicitado;

si la cantidad de veces que el valor horario almacenado (214) se actualiza con un valor horario solicitado excede un límite de solicitudes predefinido (218), iniciar un mecanismo de envío (*push*) (210) en lugar de los mensajes de solicitud, para recibir el valor horario actualizado; y

exigir una verificación de seguridad adicional de cualquier mensaje de envío (210), antes de permitir que el dispositivo de comunicaciones almacene el valor horario actualizado (212) en lugar del valor horario almacenado (214).

2. Un método como el que se reivindica en la reivindicación 1, el cual además comprende:

restablecer el conteo (218) de la cantidad de veces que se utiliza el valor horario almacenado, a un valor predeterminado, en respuesta al almacenamiento del valor horario actualizado (212), con lo que se desbloquea el suministro de servicios limitados en el tiempo, de acuerdo con el valor horario almacenado (214).

3. Un método como el que se reivindica en la reivindicación 1, en el cual los eventos de actualización ocurren a intervalos predeterminados.

4. Un método como el que se reivindica en la reivindicación 3, en el cual los intervalos predeterminados son de duración variable, duración que varía de acuerdo con una frecuencia de servicio necesaria.

5. Un método como el que se reivindica en cualquiera de las reivindicaciones 1 a 4, en el cual el valor horario actualizado se entrega en un formato cifrado.

6. Un método como el que se reivindica en cualquiera de las reivindicaciones 1 a 5, en el cual el evento de actualización es el resultado de un mensaje de difusión emitido por la red de comunicaciones.

7. Un método como el que se reivindica en cualquiera de las reivindicaciones anteriores, en el cual la red de comunicaciones es una red de comunicaciones inalámbrica.

8. Un método como el que se reivindica en cualquiera de las reivindicaciones anteriores, el cual además comprende:

mientras el dispositivo de comunicaciones permanece desconectado de la red, llevar un registro (220) de las veces que el valor horario almacenado (214) se utiliza para determinar el acceso al servicio limitado en el tiempo; y

cuando el dispositivo de comunicaciones se conecta a la red, transmitir el registro (224) a un servidor de registro (102), lo que permite consolidar el uso del servicio limitado en el tiempo.

9. Un método como el que se reivindica en cualquiera de las reivindicaciones anteriores, en el cual el servicio limitado en el tiempo tiene acceso a contenido protegido por DRM, acceso a DRM que está limitado por condiciones temporales, de modo tal que el método facilita la validación sin conexión de los derechos de acceso.

10. Un método como el que se reivindica en cualquiera de las reivindicaciones anteriores, el cual además comprende:

obtener un primer valor horario local TL0 de un origen local;

cuando se necesite un valor horario actualizado y no se pueda acceder a un valor horario proveniente de la red de comunicaciones, calcular un valor horario actualizado de modo local, obteniendo un segundo valor horario actual local TL1 del origen local; y

comprobar que el TL1 sea mayor que el TL0 y actualizar el valor horario almacenado (214), incrementando el valor horario almacenado por la diferencia entre el primer y el segundo valor horario local.

11. Un módulo seguro (108) para proporcionar valores horarios de confianza a un dispositivo de comunicaciones, dispositivo de comunicaciones que se puede emplear para conectarse a una red de comunicaciones (102,104) y que incluye medios de acceso a servicios para proporcionar acceso a servicios limitados en el tiempo, módulo seguro que incluye:

un medio de almacenamiento seguro para almacenar un valor horario (214), valor horario que es necesario para determinar el acceso a un servicio limitado en el tiempo; y

un medio de conteo (212), para contar la cantidad de veces que el valor horario almacenado (214) se utiliza para determinar el acceso al servicio limitado en el tiempo, mientras el módulo seguro se encuentra desconectado de la red de comunicaciones;

donde el medio de acceso a servicios solo proporciona acceso a dichos servicios limitados en el tiempo de acuerdo con el valor horario almacenado, si la cantidad de ocasiones en las que se ha utilizado el valor horario almacenado no excede un límite de uso predefinido;

el cual módulo seguro (108) comprende además:

un medio de interfaz para recibir un valor horario actualizado (212) en un evento de actualización mientras el módulo seguro se encuentra conectado a la red de comunicaciones (102,104), evento de actualización que es resultado de un mensaje de solicitud (210) emitido por el dispositivo de comunicaciones, y donde el medio de interfaz se puede emplear para activar un evento de actualización (210) mientras el módulo seguro se encuentra conectado, con lo que se fuerza la recepción de un valor horario actualizado (212);

un medio de comparación para comparar el valor horario actualizado (212) con el valor horario almacenado (214) en el medio de almacenamiento seguro, una vez recibido el valor horario actualizado,

un medio de conteo de solicitudes, para contar la cantidad de ocasiones en las cuales el valor horario almacenado (214) se actualiza con un valor horario solicitado;

un medio de iniciación, para iniciar un mecanismo de envío (210) en lugar de un mecanismo de solicitud, si la cantidad de veces que el valor horario almacenado (214) se actualiza con un valor horario solicitado excede un límite de solicitudes predefinido (218);

un medio para verificar la seguridad, para llevar a cabo una verificación de seguridad adicional de cualquier mensaje de envío (210), antes de permitir que el dispositivo de comunicaciones almacene el valor horario actualizado (212) en lugar del valor horario almacenado (214); y

un medio de escritura segura, para almacenar el valor horario actualizado (212) en lugar del valor horario almacenado (214), solo si el valor horario actualizado es más reciente que el valor horario almacenado.

12. Un módulo seguro (108) como el que se reivindica en la reivindicación 11, el cual además comprende:

un medio de restablecimiento, para restablecer el medio de conteo (218) a un valor predeterminado en respuesta al almacenamiento del valor horario actualizado (212), con lo que se desbloquea el suministro de servicios limitados en el tiempo, de acuerdo con el valor horario almacenado.

13. Un módulo seguro (108) como el que se reivindica en la reivindicación 11, en el cual los eventos de actualización (210) ocurren a intervalos predeterminados.

14. Un módulo seguro como el que se reivindica en la reivindicación 13, en el cual los intervalos predeterminados son de duración variable, duración que varía de acuerdo con una frecuencia de servicio necesaria.

15. Un módulo seguro como el que se reivindica en cualquiera de las reivindicaciones 11 a 14, en el cual el valor horario actualizado (212) se entrega en un formato cifrado.

16. Un módulo seguro como el que se reivindica en cualquiera de las reivindicaciones 11 a 15, en el cual el evento de actualización es el resultado de un mensaje de difusión emitido por la red de comunicaciones.

17. Un módulo seguro como el que se reivindica en cualquiera de las reivindicaciones 11 a 16, en el cual la red de comunicaciones es una red de comunicaciones inalámbrica.

18. Un módulo seguro como el que se reivindica en cualquiera de las reivindicaciones 11 a 17, el cual además comprende:

un medio de registro para llevar un registro (220) de las veces que el valor horario almacenado se utiliza para determinar el acceso al servicio limitado en el tiempo mientras el dispositivo de comunicaciones permanece desconectado de la red;

donde el medio de interfaz se puede emplear asimismo para transmitir el registro (220) a un servidor de registro (102) cuando el dispositivo de comunicaciones se conecta a la red, lo que permite consolidar el uso del servicio limitado en el tiempo.

19. Un módulo seguro como el que se reivindica en cualquiera de las reivindicaciones 11 a 18, en el cual el servicio limitado en el tiempo tiene acceso a contenido protegido por DRM, acceso a DRM que está limitado por condiciones de tiempo, de modo tal que el módulo facilita la validación sin conexión de los derechos de acceso.

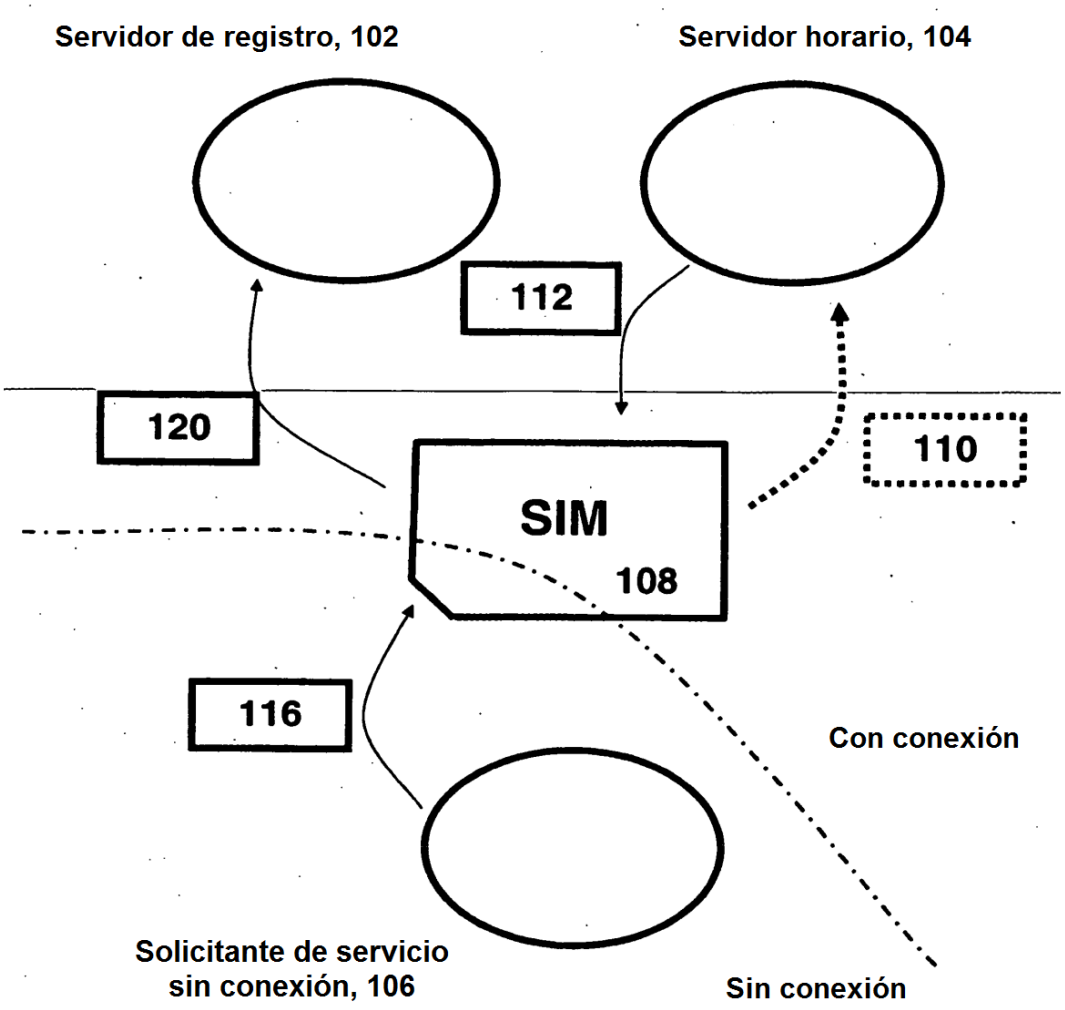
Servidor de registro, 102
Servidor horario, 104
112
120
110
SIM
108
116
Con conexión
Solicitante de servicio
sin conexión, 106
Sin conexión

Fig 1

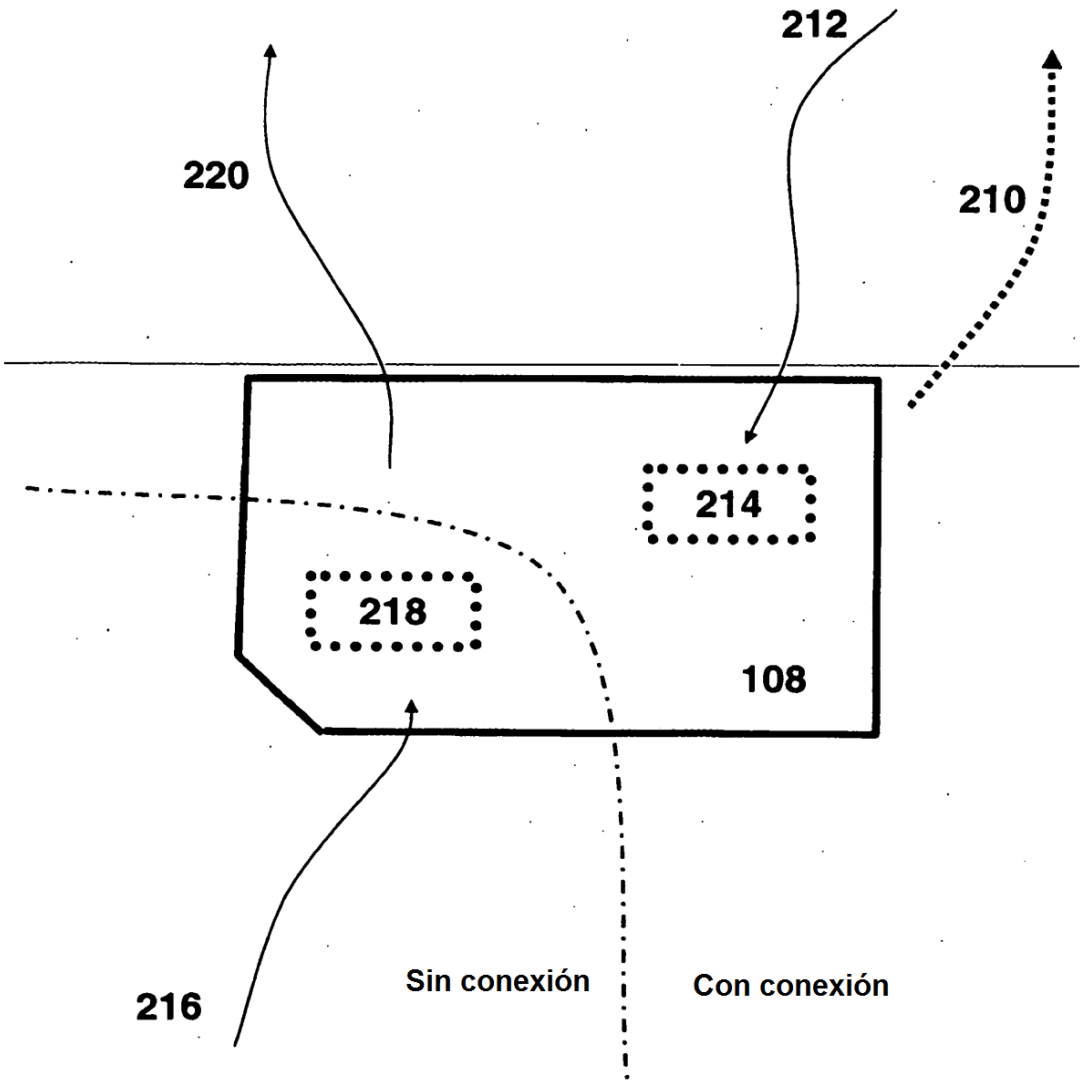

Fig 2