(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 672 988**

(51) Int. CI.:

G01S 19/03 (2010.01)
G01S 19/21 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.07.2014 PCT/EP2014/064285**

(87) Fecha y número de publicación internacional: **15.01.2015 WO15004011**

(96) Fecha de presentación y número de la solicitud europea: **04.07.2014 E 14735575 (4)**

(97) Fecha y número de publicación de la concesión europea: **11.04.2018 EP 3019891**

(54) Título: **Señales de radionavegación por satélite firmadas digitalmente**

(30) Prioridad:

09.07.2013 EP 13175821

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.06.2018

(73) Titular/es:

THE EUROPEAN UNION, REPRESENTED BY THE EUROPEAN COMMISSION (100.0%)
Rue de la Loi, 200
1049 Brussels, BE

(72) Inventor/es:

FERNANDEZ-HERNANDEZ, IGNACIO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Señales de radionavegación por satélite firmadas digitalmente

Campo técnico

La presente invención se refiere, en general, a la autenticación de señales de radionavegación por satélite, por ejemplo, señales del Sistema Global de Navegación por Satélite (GNSS) o señales del Sistema de Aumentación Basado en Satélites (SBAS). Específicamente, la invención se refiere a un método para firmar digitalmente dichas señales, y a un método de autenticación que usa las firmas digitales.

Antecedentes técnicos

Durante la última década, la creciente dependencia del GNSS (más particularmente: GPS), por parte de las aplicaciones civiles, ha generado preocupación en torno a la seguridad del GNSS. Esta cuestión ha sido abordada exhaustivamente en el denominado Informe Volpe (*Vulnerability Assessment of the Transport Infrastructure Relying on the GPS* – 29 de agosto de 2001 – Centro Nacional de Sistemas de Transporte John A. Volpe) en relación con el sector del transporte. En la comunidad dedicada a la localización ha surgido gradualmente la demanda de autenticación de señales de OS (servicio abierto). La dependencia mundial del GPS para aplicaciones civiles, algunas con aplicaciones de seguridad, se ha considerado como un problema para el programa durante los últimos años. Todavía no se ha implementado ninguna autenticación civil, aunque las comunidades de investigadores han planteado algunas propuestas. La Comisión Europea y la Agencia del GNSS Europeo están estudiando la incorporación de Autenticación de OS a la hoja de ruta del servicio Galileo.

El término “autenticación” en el dominio de la navegación por satélite se refiere, en general, a la autenticidad de una posición calculada a partir de señales de satélites de navegación. Para autenticar una posición, es necesario garantizar la autenticidad de las señales usadas en el cálculo de la posición y, además de eso, el receptor debe cerciorarse de que el proceso interno para calcular esta posición no ha sido falseado. En el contexto del presente documento, autenticación significa principalmente autenticación de señales. Las dos informaciones principales que extrae un receptor a partir de las señales de radionavegación por satélite son la información de posición y tiempo del satélite (contenidas en el mensaje de navegación), y el tiempo de llegada de la señal (que, en la mayoría de receptores, se obtiene por mediciones de fase de código). Por lo tanto, la autenticación de señales de radionavegación se refiere a:

- la confirmación de la autenticidad y la integridad de los datos transmitidos desde el satélite.
- la confirmación de la autenticidad del tiempo de llegada de la señal medido por el receptor.

La autenticación puede garantizar un cierto nivel de seguridad contra las amenazas que puede plantear un atacante para falsear las señales de radionavegación lo cual conduce a posiciones falsas. Estas amenazas se dividen habitualmente en interferencias deliberadas (*jamming*), suplantación de señales (*spoofing*) y retransmisión de señales falseadas (*meaconing*).

Los ataques con interferencias deliberadas no se pueden desviar fácilmente modificando las propiedades de la señal (si no es aumentando significativamente la potencia de transmisión), por lo que este documento no se centra en ellos. Los ataques con interferencias deliberadas conducen a una denegación de la posición, mientras que los ataques por suplantación de identidad o retransmisión de señales falseadas conducen a una posición errónea, con consecuencias potencialmente más peligrosas.

En el pasado se han presentado diversos planteamientos para la autenticación de señales de radionavegación por satélite.

El artículo “Signal Authentication – A Secure Civil GNSS for Today”, de Sherman Lo et al., publicado en la versión de septiembre/octubre de 2009 de InsideGNSS da a conocer un método de autenticación de señales GNSS que se basa en el hecho de que la frecuencia L1 del GPS es portadora de señales tanto de código C/A como de código P(Y) (cifradas), transmitidas en cuadratura de fase. El método aprovecha, además, el hecho de que la secuencia de código P(Y) recibida en una primera ubicación (la ubicación de un receptor, cuya posición se va a autenticar) es idéntica a la secuencia de código P(Y) recibida en una segunda ubicación (la ubicación de un receptor monitorizador), si se tiene en cuenta la diferencia de los tiempos de la señal del satélite al receptor. La presencia de un pico de correlación en las secuencias de código P(Y) registradas en las dos ubicaciones establece la autenticidad de la señal (si se supone que ambos receptores no están simultáneamente dentro del alcance de recepción del mismo atacante por suplantación de señales). En los documentos US 2009/0195443 y US 2009/0195354 se dan a conocer, además, aspectos específicos de este método.

El extracto “PROSPA: Open Service Authentication”, de M. Turner, A. Chambers, E. Mak, Astrium UK; E. Aguado, B. Wales, M. Dumville, NSL, UK; P. Lindsay, UKSA, UK, disponible en línea en: http://www.ion.org/meetings/abstracts.cfm?paperID=244, se refiere al denominado sistema PROSPA. El sistema PROSPA final incluirá un “generador de fragmentos” situado en centros seguros. El generador de fragmentos será,

esencialmente, un receptor PRS. Un algoritmo privativo, que no revela el código cifrado, genera fragmentos de la señal PRS cifrada. Los fragmentos se comprueban en el centro de servicio usando un receptor de validación de fragmentos, y, si se confirma que son buenos, se distribuyen a los receptores de los usuarios por medio de un canal de comunicaciones. A continuación, los receptores de usuario pueden autenticar las señales de servicio abierto llevando a cabo una correlación alineada en el tiempo con el fragmento PRS. Una correlación fuerte revela que la señal PRS está presente, y, por tanto, la señal es auténtica y adecuada para usarse.

La patente de Estados Unidos 5.754.657 da a conocer un método de autenticación o validación en el que el receptor cuya posición va a ser validada o invalidada forma una “señal de datos aumentados” que comprende datos de señal sin procesar así como la posición y el tiempo aseverados. La señal de datos aumentados se transmite a una estación central, la cual, esencialmente, comprueba si los datos sin procesar son consistentes con la posición y el tiempo aseverados, así como con las señales difundidas de manera general por los satélites.

La solicitud de patente de Estados Unidos 2013/0060955 da a conocer un sistema y un método para la autenticación de ubicaciones. Un cliente (receptor) está configurado para recibir el mensaje de navegación de cada una de las señales de satélite de navegación. El cliente estima bits de datos de navegación contenidos en los mensajes de navegación, y calcula una firma que depende de los tiempos de llegada de los mensajes de navegación (por ejemplo, la firma puede ser una suma XOR de bits de los mensajes de navegación). Un servidor de autenticación usa la ubicación aseverada del cliente (o PVT) para estimar la firma del mismo. La validez o invalidez de la ubicación aseverada se determina sobre la base de una comparación de la firma del cliente y la estimación de la misma calculada por el servidor.

La solicitud de patente de Estados Unidos 2010/0283671 se refiere a un receptor que recibe una pluralidad de señales que están moduladas con una portadora común, originándose cada una de las señales en una fuente diferente y experimentando un retardo de tránsito y un desplazamiento de frecuencia Doppler antes de llegar al receptor, estando relacionados el retardo de tránsito y el desplazamiento de frecuencia Doppler con la posición y el movimiento de cada una de las fuentes respectivas. El receptor incluye medios, tales como una antena direccional, para garantizar que las señales recibidas son de buena fe, o, por lo menos, no están sujetas a la misma señal o señales falsas a las cuales puede estar sujeto un segundo receptor.

La solicitud de patente de Estados Unidos 2009/0316900 da a conocer un sistema de cifrado y descifrado de datos que “geocifra” de manera segura datos utilizando señales de navegación dependientes de la ubicación.

La solicitud de patente internacional WO 2011/157554 A1 se refiere a un método de provisión de una indicación autenticable de tiempo y ubicación usando un receptor de señales de radionavegación. El método comprende recibir señales de radionavegación difundidas de forma general desde una pluralidad de fuentes de señales de radionavegación, de modo que al menos algunas de las señales de radionavegación contienen uno o más testigos criptográficos protegidos por cifrado, actualizándose ocasionalmente los testigos criptográficos. El receptor, mediante descifrado, recupera los testigos criptográficos a partir de las señales de radionavegación que los contienen. A continuación, el receptor determina datos de posicionamiento, que representan su posición geográfica y tiempo, sobre la base de las señales de radionavegación recibidas. El receptor genera un código de autenticación digital usando una función criptográfica que toma como entradas al menos los datos de posicionamiento y los testigos criptográficos recuperados, y produce un paquete de datos que incluye una primera parte que contiene los datos de posicionamiento y una segunda parte que contiene el código de autenticación digital.

El documento “Practical Cryptographic Civil GPS Signal Authentication” de Kyle Wesson, Mark Rothlisberger, y Todd Humphreys, NAVIGATION, Volumen 59, edición 3, páginas 163 a 248, menciona una implementación de la técnica denominada autenticación de mensajes de navegación (NMA), técnica de acuerdo con la cual el mensaje de navegación de baja velocidad se cifra o firma digitalmente, permitiendo que un receptor verifique el Segmento de Control GPS generó los datos.

El documento de trabajo “Authenticating GNSS – Proofs against Spoofs – Part 2” de Guenter W. Hein, Felix Kneiss I, Jose-Ang el Avila-Rodriguez, y Stefan Wallner, en InsideGNSS, septiembre/octubre de 2007, propone métodos de NMA normalizados para la autenticación de señales Galileo.

Problema técnico

Es un objetivo de la presente invención posibilitar la autenticación de señales de radionavegación por satélite con un buen nivel de seguridad.

Descripción general de la invención

Un primer aspecto de la invención se refiere a un método para firmar digitalmente señales de radionavegación por satélite. El método comprende:

- controlar un primer satélite de radionavegación de tal manera que el satélite introduce bits impredecibles, por ejemplo, una secuencia de bits aleatoria o seudoaleatoria, en un primer mensaje de navegación difundido de manera general por el primer satélite, por ejemplo, cuando el primer satélite no está enlazado en ese

momento con el segmento de misión terrestre;

- generar una firma digital de una sección de mensaje de navegación que contiene los bits impredecibles, mediante la aplicación de una función *hash* criptográfica sobre el mensaje de navegación y un cifrado subsiguiente;
- transmitir la firma digital a un segundo satélite de radionavegación enlazado con el segmento de misión terrestre y
- controlar el segundo satélite de tal manera que introduce la firma digital en un segundo mensaje de navegación difundido de forma general por el segundo satélite.

Tal como observarán aquellos versados en la materia, la presente invención se basa en un concepto nuevo, el cual se puede considerar como autenticación “cruzada” de mensajes de navegación, ya que la firma digital que autentica un mensaje de navegación no se envía como parte del mismo mensaje, sino como parte de un mensaje de navegación difundido de forma general poco tiempo (por ejemplo, unos pocos segundos) después por otro satélite. El método se basa en el siguiente principio:

- generación y transmisión de bits aleatorios o seudoaleatorios (impredecibles) periódicamente desde satélites, que no necesitan estar conectados al segmento de misión terrestre en el momento que difunden de forma general su mensaje de navegación.
- generación de firmas digitales para los datos provenientes de estos satélites, y su transmisión a través de otros satélites.

Un ataque no puede suplantar fácilmente el mensaje de navegación en la medida en la que contiene un patrón de bits impredecible que se verifica, de manera simultánea o unos pocos segundos más tarde, a través de una firma digital.

Debe indicarse que la expresión “bits impredecibles” significa bits cuyos valores no son predecibles por receptores de usuario. Por lo tanto, el uso de la expresión no está destinado a excluir la predictibilidad de los valores de bits por parte de la entidad (de confianza) que genera las firmas digitales.

Según una realización preferida de la invención, el mensaje de navegación del primer satélite que contiene los bits impredecibles se recibe en un receptor monitorizador o una red de receptores monitorizadores, y el mensaje de navegación recibido se usa para generar la firma digital. De acuerdo con esta realización de la invención, no es necesario que la entidad que genera la firma digital conozca de antemano los bits impredecibles. Uno de los inconvenientes de este método es su latencia inherente, la cual es debida al hecho de que el mensaje a firmar debe ser recibido primero, y a continuación, debe cargarse la firma en el satélite firmante (segundo satélite). Si los bits impredecibles son conocidos de antemano para la entidad de generación de firmas digitales (pero no para los receptores), el mensaje de navegación a firmar (proveniente del primer satélite) y la firma digital (proveniente del segundo satélite) se podrían difundir de manera general con un retardo significativamente menor o incluso simultáneamente.

Tal como se apreciará, la solución de autenticación propuesta requiere relativamente pocas modificaciones de la infraestructura normalizada de radionavegación por satélite. En el lado del sistema (por contraposición al lado del usuario), los satélites de radionavegación deben poder introducir los bits impredecibles en el mensaje de navegación. Esto se puede lograr equipando a los satélites de radionavegación con generadores de secuencias (seudo)aleatorias o cargando las secuencias (seudo)aleatorias en los satélites por medio de un enlace de comunicaciones cifrado. Además, debe preverse un receptor monitorizador o una red de receptores monitorizadores para recibir los mensajes de navegación difundidos de manera general por los satélites y para proporcionar los argumentos de la función *hash* criptográfica. Finalmente, las firmas digitales se deben cargar en los satélites que las difunden de manera general. Esto requiere una capacidad suficiente de enlace ascendente (entre el segmento de misión terrestre y los satélites de radionavegación), así como la posibilidad de introducir las firmas digitales en el mensaje de navegación.

Una constelación de satélites de radionavegación puede comprender diversos satélites no conectados, a la vez, al segmento de misión terrestre. Por consiguiente, el segundo satélite se controla, preferentemente, de tal manera que introduce un identificador en el segundo mensaje de navegación, el cual identifica el primer mensaje de navegación como aquello que ha sido firmado digitalmente. En otras palabras, si existen diversos primeros mensajes de navegación de diferentes satélites, el identificador sirve para identificar el satélite que se encontraba en el origen del mensaje de navegación en la base de la firma digital.

El primer satélite de radionavegación se puede controlar de tal manera que introduzca un primer preámbulo en el primer mensaje de navegación, precediendo a los bits impredecibles e identificando los bits impredecibles como tales. El primer preámbulo informa a los receptores de que el satélite va a transmitir los bits impredecibles. De manera similar, el segundo satélite de radionavegación se controla, preferentemente, de tal manera que introduce un segundo preámbulo en el segundo mensaje de navegación, precediendo a la firma digital e identificando la firma

digital como tal. El segundo preámbulo informa a los receptores de que el satélite va a transmitir una firma digital. Los preámbulos son útiles puesto que el rol de un satélite de radionavegación particular en la implementación del método puede cambiar a lo largo del tiempo: mientras el satélite está enlazado con el segmento de misión terrestre, transmite firmas digitales (es decir, funciona como segundo satélite), pero mientras no está enlazado al segmento de misión terrestre, transmite periódicamente sus bits impredecibles (es decir, funciona como primer satélite).

Preferentemente, la firma digital tiene una fortaleza equivalente de clave simétrica de 112 bits por lo menos, para presentar la suficiente robustez contra una búsqueda exhaustiva de claves u otros ataques.

La sección de mensaje de navegación que contiene los bits impredecibles y a la que se aplica la función *hash* y se firma, tiene preferentemente una longitud en el intervalo de 400 a 500 bits. En la señal de OS Galileo, esto se correspondería con un tiempo de transmisión no superior a 4 s.

Según una realización preferida de la invención, la sección de mensaje de navegación que contiene los bits impredecibles y a la que se aplica la función *hash* y se firma, tiene una longitud de por lo menos 448 bits, la función *hash* criptográfica es SHA-224 y el cifrado se basa en ECDSA K-233.

Si el método según el primer aspecto de la invención se implementa en el GNSS Galileo, el primer y el segundo mensajes de navegación son, preferentemente, mensajes Galileo E1 I/NAV.

El cifrado del valor *hash* de la sección del primer mensaje de navegación se lleva a cabo, preferentemente, usando una clave privada de un par de claves criptográficas, compuesto por una clave privada y una clave pública que siguen planteamientos de cifrado asimétrico. También se podría realizar siguiendo planteamientos simétricos adaptados a la autenticación del origen de los datos como autenticación tolerante a pérdidas del flujo continuo y eficiente en el tiempo (TESLA).

Un segundo aspecto de la invención se refiere a un método para autenticar señales de radionavegación por satélite abiertas, en el nivel del receptor de usuario. Ese método comprende:

- recibir, en un receptor de usuario, una primera señal de radionavegación que es portadora de un primer mensaje de navegación difundido de manera general por un primer satélite de radionavegación que puede no estar enlazado en ese momento con un segmento de misión terrestre, comprendiendo el primer mensaje de navegación una sección de mensaje de navegación que contiene bits impredecibles, por ejemplo, una secuencia de bits aleatoria o seudoaleatoria;

- recibir, en el receptor de usuario, una segunda señal de radionavegación que es portadora de un segundo mensaje de navegación difundido de forma general por un segundo satélite de radionavegación enlazado en ese momento con un segmento de misión terrestre, conteniendo el segundo mensaje de navegación una firma digital, que se supone obtenida mediante la aplicación de una función *hash* criptográfica sobre la sección de mensaje de navegación según es recibida por un receptor monitorizador o una red de receptores monitorizadores, y un cifrado subsiguiente;

- aplicar una función *hash* criptográfica sobre la sección del primer mensaje de navegación que contiene los bits impredecibles para generar un valor *hash*;

- descifrar la firma digital contenida en el segundo mensaje de navegación;

- comparar el valor *hash* con la firma digital descifrada.

Preferentemente, el receptor está configurado para considerar la primera y la segunda señales de radionavegación auténticas si el valor *hash* y la firma digital descifrada coinciden, si el receptor permanece enganchado a la primera señal de radionavegación durante la recepción del primer mensaje de navegación y si el receptor permanece enganchado a la segunda señal de radionavegación durante la recepción del segundo mensaje de navegación. El receptor puede continuar considerando la primera y la segunda señales de radionavegación auténticas mientras permanece enganchado a la primera y a la segunda señales de radionavegación, respectivamente, si no se detecta ningún salto del reloj del receptor u otras alteraciones de la señal.

Preferentemente el descifrado se lleva a cabo con una clave pública de un par de claves criptográficas.

Todavía otro aspecto de la invención se refiere a un programa de ordenador ejecutable por un receptor de señales de radionavegación por satélite, comprendiendo el programa de ordenador instrucciones que, cuando son ejecutadas por el receptor de señales de radionavegación por satélite, consiguen que el receptor de señales de radionavegación por satélite implemente el método de acuerdo con el segundo aspecto de la invención. El programa de ordenador se puede materializar en un producto de programa de ordenador que comprenda una memoria no volátil con instrucciones almacenadas en la misma, las cuales, cuando son ejecutadas por el receptor de señales de radionavegación por satélite, consiguen que el receptor de señales de radionavegación por satélite implemente el método de acuerdo con el segundo aspecto de la invención.

Breve descripción de los dibujos

A continuación se describirán, a título de ejemplo, realizaciones preferidas de la invención en referencia a los dibujos adjuntos, en los cuales:

la Fig. 1 es una ilustración esquemática del concepto que subyace tras una realización preferida de la invención según se observa desde la perspectiva del receptor (de usuario);

la Fig. 2 es una ilustración esquemática del concepto que subyace tras la realización preferida de la invención desde la perspectiva del sistema/proveedor de servicios;

la Fig. 3 es una ilustración de cómo se puede usar el mensaje Galileo E1B I/NAV para la transmisión de los bits impredecibles y las firmas digitales;

la Fig. 4 es una ilustración esquemática de una situación ejemplificativa con 6 satélites no conectados y 2 satélites conectados al segmento de misión terrestre;

la Fig. 5 es un diagrama de temporización del proceso de autenticación en un receptor en una fase de arranque;

la Fig. 6 es un diagrama de temporización del proceso de autenticación de un receptor cuando se está realizando el seguimiento de ocho satélites.

Descripción de realizaciones preferidas

A continuación se describirá, en referencia a las Figs. 1 y 2, una realización preferida del concepto de autenticación de OS propuesto. La finalidad de este concepto es proporcionar una serie de señales en el espacio autenticadas que pueden ser convertidas por un receptor GNSS en seudodistancias autenticadas, y calcular una posición autenticada. El concepto se basa en las siguientes etapas principales:

- La generación a bordo y la transmisión de bits de datos impredecibles (aleatorios o seudoaleatorios) periódicamente desde satélites (de forma temporal) no conectados al segmento de misión terrestre.
- La generación de firmas digitales para los datos provenientes de estos satélites, y su transmisión a través de satélites conectados al segmento de misión terrestre.

Un atacante no puede suplantar los datos de navegación ya que contienen información impredecible que se verifica unos pocos segundos más tarde a través de una firma digital.

La Fig. 1 ilustra el concepto propuesto como se presenta a un receptor de usuario Rx. P1, P2 y P3 representan los mensajes de navegación (o parte de ellos) de los satélites 1, 2 y 3, respectivamente. Se les denomina P siguiendo la notación estándar en criptografía, de manera que P significa “texto plano”, es decir, el texto o mensaje antes de que sea cifrado, o firmado en este caso. DS(P1), DS(P2) y DS(P3) representan las firmas digitales de P1, P2 y P3. Las firmas digitales se envían desde el satélite 4.

En la situación ilustrada, los satélites 1, 2 y 3 no están conectados al segmento de misión terrestre, lo cual significa que ninguna estación de enlace ascendente de misión terrestre está transmitiendo ningún dato a los mismos, mientras que el satélite 4 sí que está conectado.

Desde la perspectiva del receptor de usuario, la secuencia de eventos es la siguiente:

- Los satélites 1, 2 y 3 transmiten sus mensajes de navegación normales P1, P2 y P3. Estos mensajes incluyen, aparte de su contenido habitual (datos de efemérides y de reloj, datos ionosféricos, etcétera), algunos bits aleatorios o seudoaleatorios generados a bordo del satélite. Estos bits no tienen ningún significado pero son impredecibles para cualquier suplantador.
- El receptor aplica una función *hash* a P1, P2 y P3 a través de un algoritmo *hash* convencional, generando $H1^1$, $H2^2$ y $H3^3$, de manera que el superíndice indica, en este caso, que la función *hash* se corresponde con datos recibidos, respectivamente de los satélites 1, 2 y 3.
- El receptor almacena en memoria $H1^1$, $H2^2$ y $H3^3$.
- Durante los siguientes segundos, el receptor recibe secuencialmente DS1, DS2 y DS3 del satélite 4.
- El receptor comprueba la autenticidad de los datos firmados digitalmente, a través de un proceso de verificación de firma digital:
  - Descifra DS(P1), DS(P2) y DS(P3) con una clave pública previamente transmitida (Kpb), con lo cual obtiene los valores *hash* $H1^4$, $H2^4$ y $H3^4$.

- Compara $H1^1$ con $H1^4$, $H2^2$ con $H2^4$ y $H3^3$ con $H3^4$. Si todos ellos coinciden, eso significa que las señales de los satélites 1, 2, 3 y 4 son auténticas.

○ Para autenticar el tiempo de llegada (TOA) de medición de los satélites cuyos datos han sido verificados, el receptor puede llevar a cabo comprobaciones locales a través de detectores de interferencias deliberadas, detectores de saltos de reloj del receptor, consistencia de medición global.

○ Para proteger el proceso de autenticación, el receptor, preferentemente, incluye medidas contra manipulaciones indebidas, que evitan que un atacante acceda y/o controle áreas de memoria en las que se almacena información relevante para la autenticación.

○ Si las comprobaciones de autenticación resultasen satisfactorias, el receptor puede calcular una posición y un tiempo tridimensionales autenticados, sobre la base de las mediciones y los datos de al menos cuatro satélites autenticados.

Para un receptor estático, podrían usarse las mediciones de seudodistancia asociadas a bits recién autenticados, incluso si se corresponden con épocas diferentes. Para un receptor dinámico, deberían sincronizarse las mediciones de seudodistancia usadas para un cálculo de la posición. Esto significa que las señales pueden haberse autenticado hace algunos segundos. No obstante, se considera que, si las señales GNSS siguen enganchadas por los bucles de seguimiento del receptor desde la última autenticación satisfactoria, las mismas son autenticas, con una probabilidad muy alta, en el momento que se usan para el cálculo de la posición. Esto se refuerza por el hecho de que las mediciones de seudodistancia deberían ser coherentes entre sí y, en caso negativo, puede detectarse un ataque.

En contraposición a los algoritmos convencionales de firma digital, en los que hay una fuente de información que proporciona tanto el texto plano como la firma digital, la presente invención usa una autenticación cruzada, en donde el texto plano y la firma digital correspondientes se proporcionan por medio de trayectos de comunicación diferentes. Específicamente, los emisores del texto plano y el(los) emisor(es) de las firmas digitales son satélites diferentes. Siempre que el texto plano sea impredecible para el atacante, comparando el texto plano al que se ha aplicado la función *hash* y la firma digital descodificada, las dos fuentes se pueden autenticar al mismo tiempo.

Los satélites deben usar bits impredecibles que consigan que su mensaje de navegación (o parte del mismo) sea impredecible. De lo contrario, un suplantador podría simplemente reproducir el mensaje de navegación de los satélites 1, 2 y 3 mientras suplanta el tiempo de llegada de la señal lo cual conduce a un punto de posición potencialmente suplantado.

La Fig. 2 ilustra el concepto según se ve desde la perspectiva del sistema/proveedor de servicios. La secuencia de eventos es la siguiente:

○ Los satélites 1, 2 y 3 transmiten sus mensajes de navegación normales P1, P2 y P3. Estos mensajes incluyen, aparte de su contenido habitual (efemérides y relojes, ionosfera, etcétera) algunos bits aleatorios o seudoaleatorios generados a bordo del satélite. Estos bits no tienen ningún significado pero son impredecibles para cualquier suplantador.

○ P1, P2 y P3 son recibidos en tierra por un receptor (denominado receptor monitorizador puramente para diferenciarlo de los receptores de usuario), o una red de receptores monitorizadores, que transmiten los datos a un generador de firmas digitales DSG.

○ El generador de firmas digitales DSG aplica la función *hash* a P1, P2 y P3 obteniendo H1, H2 y H3, y genera firmas digitales DS1, DS2 y DS3 cifrando los valores *hash* a través de una clave privada (Kpv).

○ Las firmas digitales se transmiten periódicamente en el Segmento de Misión Terrestre (GMS) operativo del GNSS en cuestión.

○ Un Mecanismo de Generación de Mensajes (MGF) incorpora los bits de DS en el mensaje de navegación, y lo transmite a una Estación de Enlace Ascendente (ULS) que lo envía por enlace ascendente al satélite conectado 4.

○ El satélite 4 transmite las firmas digitales durante los siguientes segundos.

Aspectos como la geometría satelital, la longitud de los mensajes, la latencia de las firmas y cuestiones de sincronización se explican de forma más detallada posteriormente.

La arquitectura ilustrada en la Fig. 2 contempla un proceso de generación de firmas digitales fuera del perímetro del segmento de misión terrestre del GNSS. Aunque esto minimizase el impacto de la implementación de la invención sobre el segmento de misión terrestre, también sería posible integrar el(los) receptor(es) monitorizador(es) y el generador de firmas digitales DSG en el segmento de misión terrestre.

A continuación, se ilustrará adicionalmente la invención en referencia a un ejemplo específico, en el cual la invención sirve para autenticar la señal E1 OS Galileo.

La fortaleza equivalente de clave simétrica de una firma digital, según recomienda NIST para el periodo 2011 a 2030, equivale a por lo menos 112 bits (longitudes superiores como, por ejemplo, 160 bits, pueden ser más prudentes, y pueden considerarse en realizaciones futuras). Para lograr una fortaleza de clave simétrica de 112 bits,

- RSA requeriría una firma de 2.048 bits. Dado que el rendimiento del sistema, especialmente en términos del tiempo hasta la primera autenticación (TTFA) y del tiempo entre autenticaciones (TBA), es muy sensible a la longitud de las firmas, el RSA no parece la mejor opción.
- El DSA requeriría una firma de 448 bits, lo cual es más asequible para una transmisión en el mensaje de navegación.
- ECDSA requeriría una firma de un tamaño similar al DSA, aunque el ECDSA es menos complejo computacionalmente.
- Los métodos TESLA implicarían la transmisión de una clave de 112 bits con un cierto retardo, y un código de autenticación de mensaje (MAC) completo o truncado de un tamaño similar o menor, lo cual hace que este planteamiento sea potencialmente adecuado como realización de la invención propuesta.

Debido a su madurez y a la aceptación por parte de la comunidad criptográfica, así como por sus características técnicas, el ECDSA parece actualmente una buena opción. En particular, para las explicaciones posteriores se usará el ECDSA K-233. Por lo que respecta al algoritmo *hash* y la longitud del valor *hash*, puede usarse el SHA-2 (con una clave de 224 bits, o SHA-224), en la medida en la que cumple el requisito de fortaleza de seguridad de 112 bits.

En este ejemplo, se propone el SHA-224 con un algoritmo ECDSA K-233 con una longitud de firma digital de 466 bits. No obstante, debe indicarse que podrían usarse otros algoritmos *hash* y otros algoritmos de cifrado, siempre que el nivel de seguridad de la firma sea satisfactorio y la longitud de la firma digital sea compatible con el espacio disponible en los mensajes de navegación.

La longitud del mensaje al que se va a aplicar la función *hash* debe ser por lo menos 2 veces la salida *hash*. Con un algoritmo *hash* SHA-224, deberían firmarse por lo menos 448 bits. Esta cantidad de bits se puede transmitir en 4 segundos sobre la señal E1B del Galileo; esta duración se corresponde con 2 páginas nominales de datos (para obtener información sobre el mensaje de navegación E1B Galileo, puede hacerse referencia al Documento de Control de Interfaz de Señales en el Espacio, de Servicio Abierto [OS SIS ICD], Edición 1.1, septiembre de 2010, disponible en línea en: http://ec.europa.eu/enterprise/policies/satnav/galileo/files/galileo-os-sis-icd-issue1-revision1_en.pdf).

Uno de los requisitos sobre los segmentos del mensaje a firmar es que los mismos deben variar de un mensaje al siguiente en por lo menos 1 bit, con el fin de evitar la repetición de la misma firma. Puesto que parte de los bits firmados es aleatoria o seudoaleatoria, las firmas variarán de manera impredecible de una a la siguiente.

Una de las cuestiones que surge es si se deberían firmar todos los datos de los mensajes de navegación, o solamente parte de los mismos, o si, verificando la autenticidad de unos pocos bits periódicamente, el resto de los bits se puede considerar como auténtico. Este aspecto requiere de una solución de compromiso. Si la transmisión de los datos a firmar tarda mucho tiempo, la latencia de autenticación, el tiempo hasta la primera autenticación y el periodo requerido de recepción de datos sin errores serán mayores. Por otra parte, la autenticación puede verse reducida para usuarios sin condiciones buenas de visibilidad y seguimiento de forma continua, en caso de que se detecten errores de bit de navegación. Por otro lado, si se autentican solamente unos pocos bits del mensaje de navegación, la solución de navegación puede perder parte de su robustez, en la medida en la que un suplantador podría desarrollar otro tipo de ataques en los que algunos bits de navegación (aquellos no autenticados), o su medición de seudodistancia asociada, se falsean mientras que otros no (los autenticados). Este tipo de amenaza se considera actualmente complicada, ya que sería necesario falsear la posición del usuario modificando los parámetros de efemérides (órbitas y relojes) de varios satélites, de una manera continua y coherente que prediga la trayectoria del usuario:

- En la medida en la que las órbitas satelitales se proporcionan usando parámetros keplerianos (véase el OS SIS ICD), resulta muy difícil (cuando no imposible) generar conflictos de datos de efemérides para varios satélites, que conduzcan a una posición coherentemente suplantada durante varios minutos.
- Por lo que respecta a los parámetros de reloj (af0, af1, af2 en el OS SIS OCD), estos podrían ser los más sencillos de modificar ya que los mismos simplemente se añaden a la medición de la seudodistancia. No obstante, para generar de forma continua y coherente una posición errónea en el receptor, es necesario cambiar sus valores gradualmente. Si esto es así, el usuario puede darse cuenta fácilmente comprobando la velocidad de actualización de los errores de reloj de satélite, ya que la navegación Galileo (órbitas y relojes) no se puede actualizar con un periodo inferior a 10 minutos, y, habitualmente, se actualizará con un periodo superior de hasta 100 minutos.

- Si el receptor se enganchase a una señal falseada que se enciende y apaga simplemente para sustituir los bits predecibles, esto podría detectarse por medio de una discontinuidad en el nivel de la señal (por ejemplo, en el controlador de ganancia automática a través de un detector de J/N). No obstante, la ausencia de esta característica de detección puede conducir a una realización preferida en la que se firman los datos de navegación principales de los satélites (órbitas y relojes).

- Si un suplantador pretendiese falsear la posición influyendo en el ToA (tiempo de llegada) de los periodos no autenticados de la señal, esto llevaría a una pérdida frecuente de enganche de los bucles de seguimiento que podría ser detectada fácilmente como ataque de suplantación.

Para la implementación del presente ejemplo, se supone que, para garantizar que la señal transmitida es auténtica, se requieren solamente unos pocos segundos de datos autenticados periódicamente. Por consiguiente, en lo sucesivo, la sección de mensaje de navegación que se firma se corresponde con dos páginas de datos de navegación del mensaje E1B I/NAV del Galileo (500 bits en total, transmitidos durante 4 s).

En el caso de 4 satélites descrito en referencia a las Figs. 1 y 2, el satélite conectado 4 transmite firmas digitales solamente de secciones de mensaje transmitidas por los satélites no conectados 1, 2 y 3, pero no firma una de sus propias secciones de mensaje. Esto no se implementa explícitamente en el ejemplo aunque otra realización podría incluir el caso en el que la firma digital se basa en el valor *hash* no solamente del mensaje de navegación de un satélite no conectado sino en ciertos parámetros de navegación básicos del satélite 4, como, por ejemplo, relojes y órbitas. En una implementación de este tipo, el satélite 4, según las Figuras 1 y 2, transmitiría DS(P1, P4), DS(P2, P4), DS(P3, P4).

De acuerdo con el OS SIS OCD Galileo, una trama completa del mensaje I/NAV dura 720 s. Cada trama está compuesta por 24 subtramas de 30 segundos cada una de ellas. Cada subtrama contiene 15 páginas denominadas nominales. Cada página nominal está compuesta por una página “par” y una página “impar”, que tienen, cada una de ellas, una duración de 1 segundo. Las páginas “impares” contienen datos de palabras (efemérides, almanaques, etcétera) más algunos campos adicionales: “Reservado 1”, SAR, de reserva, CRC y “Reservado 2”. Las páginas “pares” contienen principalmente los datos de palabras.

Una de las características del I/NAV es que se prevé que sea enviado en señales tanto E1B como E5b. Este ejemplo se centra solamente en el E1B. Queda en el aire si el servicio de autenticación se proporciona también en el E5b. No obstante, debe indicarse que, si se implementa la misma autenticación cruzada de mensajes de navegación en el E5b y en el E1B, las secuencias de bits aleatorias o seudoaleatorias se deben seleccionar de manera independiente entre sí. Debe evitarse, por ejemplo, que la secuencia aleatoria o seudoealeatoria en el E1B no sea simplemente una copia idéntica retardada (o adelantada) de la secuencia en el E5b.

En el ejemplo de la ilustración, las secuencias de bits aleatorias o seudoaleatorias así como las firmas digitales (longitud supuesta: 466 bits) se transmiten en el campo “Reservado 1” del mensaje I/NAV. El campo “Reservado 1” proporciona 40 bits libres cada página nominal, es decir, cada 2 segundos, o 20 bps por término medio. Actualmente, el campo “Reservado 1” no se usa. En su lugar, el sistema envía todos los bits fijados a cero.

Merece la pena indicar que los datos de “Reservado 1” estaban destinados a inyectarse en el segmento terrestre a través de una fuente externa conectada en tiempo real al sistema. Esta característica permite proporcionar los datos de autenticación (es decir, las firmas digitales calculadas) al segmento terrestre sin ninguna modificación sobre este último, aparte de hacer que el enlace de “Reservado 1” esté disponible.

El uso del campo “Reservado 1” permite transmitir los datos de autenticación (o bien la secuencia aleatoria o seudoaleatoria o bien un trozo de una firma digital) cada 2 segundos desde cada satélite. Puesto que el campo “Reservado 1” está presente en todas las páginas nominales de cada subtrama, la latencia del sistema para la transmisión de una firma digital se puede mantener a un valor pequeño.

Si se usa el mismo campo de datos dentro del mensaje de navegación para la transmisión de la secuencia de bits aleatoria o seudoaleatoria y las firmas digitales, es necesario que los receptores (de usuario) dispongan de la posibilidad de diferenciar entre una secuencia de bits aleatoria o seudoaleatoria y una firma digital. Específicamente, el campo “Reservado 1” debe permitir que un receptor diferencie los siguientes casos:

1) Un satélite no está conectado al segmento de misión terrestre y enviando bits aleatorios o seudoaleatorios.

2) Un satélite está simplemente conectado a tierra esperando la sincronización con el generador de firmas digitales DSG y la transmisión de una nueva firma.

3) Un satélite está conectado y comenzando a transmitir una firma.

4) Un satélite está conectado y ya está transmitiendo una firma.

Para lograr esto, el campo “Reservado 1” se define de la manera siguiente:

1) Mientras no está conectado a tierra, un satélite generará los siguientes bits a bordo y los enviará:

   a) Un preámbulo (igual para todos los satélites desconectados) que notifica que el satélite transmisor no está conectado al segmento de misión terrestre y, por tanto, no está transmitiendo una firma digital, sino simplemente bits aleatorios o seudoaleatorios.

   b) Bits aleatorios o seudoaleatorios.

2) Cuando se acaba de conectar, y durante los pocos segundos antes de la sincronización con el generador de firmas digitales DSG, el satélite no habrá recibido todavía los datos de firma digital del segmento de misión terrestre. Por lo tanto, el satélite enviará un preámbulo diferente, que notifica a los receptores que se va a transmitir una firma, y, a continuación, algunos bits aleatorios o seudoaleatorios. El envío de la secuencia de bits aleatoria o seudoaleatoria en esta fase permite la autenticación efectiva si se da el caso que otro satélite está firmando al satélite recién conectado.

3) Cuando comienza a transmitir una firma, el satélite enviará:

   a) Un preámbulo (igual para todos los satélites conectados) que notifica a los receptores que se va a transmitir una firma digital

   b) El ID de satélite correspondiente al mismo, cuyo mensaje I/NAV está siendo firmado.

   c) Los primeros bits de la firma digital. (Cada firma digital abarca diversas páginas nominales del mensaje I/NAV).

4) Mientras ya está transmitiendo una firma, el satélite dedicará los 40 bits de “Reservado 1” a la transmisión de la firma digital. Los receptores podrán identificar esta situación debido a la ausencia de cualquiera de los preámbulos recién mencionados.

La definición de este campo “Reservado 1” a nivel de bits se presenta en la Fig. 3, en la cual Preámbulo-NC significa “Preámbulo-No-Conectado”, es decir, el preámbulo del satélite establece que el satélite no está conectado. Preámbulo-S significa “Preámbulo-Sincronización”, es decir, el preámbulo establece que el satélite se está sincronizando con el generador de firmas digitales DSG e iniciará la transmisión de la firma digital en unos pocos segundos. Preámbulo-C significa “Preámbulo-Conectado”, es decir, el preámbulo indica que el satélite está comenzando a transmitir una firma. La siguiente tabla presenta un resumen del uso de bits con la implementación propuesta. Podrían añadirse bits adicionales para evitar casos de colisión en los cuales una parte de una firma digital coincida con un preámbulo, o para añadir robustez a errores de recepción de bits a través de técnicas de codificación de canales dedicados.

PARÁMETROS DE DISEÑO	
INAV – Satélites conectados	
INAV – preámbulo [bits]	8
INAV – ID de sat [bits]	6
número de Ids de sat posibles	64
INAV – Satélites no conectados	
INAV – preámbulo [bits]	8
INAV – bits aleatorios o seudoaleatorios por palabra	32
FIRMA DIGITAL	
Longitud de firma digital total [bits]	466
INAV bits requeridos para enviar la firma	480
INAV páginas nominales requeridas para enviar la firma	12
INAV – bits libres	0
Duración de la transmisión de la firma [s]	24

La tabla muestra que una firma digital completa se puede transmitir en 24 segundos. Mientras el satélite está conectado, se pueden transmitir firmas de manera continua. Por lo tanto, un satélite conectado puede enviar 4 firmas digitales cada 96 segundos. Si un receptor está recibiendo datos de dos satélites conectados, lo cual es un escenario probable en condiciones de buena visibilidad, y la transmisión de datos está sincronizada óptimamente escalonando los tiempos de inicio de las transmisiones de firmas digitales desde los dos satélites, un receptor podría recibir una firma digital nueva cada 12 segundos. Debe indicarse también que, haciendo que los bits impredecibles sean predecibles para el generador de firmas digitales, por ejemplo, generando una secuencia seudoaleatoria a partir de un valor semilla conocido por el segmento terrestre, la latencia se podría reducir significativamente en la medida en la que el generador de firmas digitales podría transmitir las firmas digitales al mismo tiempo que el usuario recibe los datos para firmar.

Para ilustrar el funcionamiento de la invención y para presentar una valoración preliminar del rendimiento en un ejemplo concreto, son necesarias algunas consideraciones en relación con la latencia del sistema. La siguiente tabla presenta estas consideraciones.

LATENCIA DEL SISTEMA	
Transmisión de mensajes desde receptores monitorizadores al centro de control [s]	1
Generación de firmas digitales en el mecanismo de DSG [s]	1
Transmisión de firma desde el mecanismo de DSG al segmento de misión terrestre	1
Latencia del GNSS (tiempo entre la recepción de la firma en el segmento de misión terrestre y el inicio de la transmisión de la firma por el satélite)	5
latencia total del proceso [s] con las consideraciones anteriores	8

La latencia total del sistema es 8 segundos. Este es el tiempo que tardará el generador de firmas digitales en saber que un satélite está conectado y que puede comenzar a enviar firmas. Durante ese tiempo, se enviará el "Preámbulo-S". Las anteriores latencias son estimaciones muy conservadoras, teniendo en cuenta que la generación de firmas y su transmisión al segmento de misión terrestre se pueden realizar en un tiempo muy inferior a 2 segundos. Con estas consideraciones, el tiempo que transcurre entre la recepción de un flujo continuo de bits a firmar y la recepción de la firma correspondiente es 32 segundos (latencia de 8 s + tiempo de transmisión de firma de 24 s).

En lo que sigue se analizará el rendimiento, principalmente en términos de aspectos relacionados con la temporización, en el caso de un receptor que funciona en modo autónomo (es decir, no asistido) bajo condiciones de cielo abierto. Las consideraciones (ilustradas en la Fig. 4) del caso de uso autónomo utilizadas en el análisis son:

- 8 satélites Galileo (numerado del 1 al 8) están a la vista del receptor.
- De ellos, 2 satélites están conectados al segmento de misión terrestre (satélites 3 y 6) y 6 satélites no están conectados (satélites 1, 2, 4, 5, 7 y 8).
- El satélite 3 firma los satélites 1, 2, 4 y 5. El satélite 6 firma los satélites 4, 5, 7 y 8. Esto significa que hay un solapamiento de 2 satélites (4 y 5) y la firma para estos satélites se recibe tanto del satélite 3 como del satélite 6. Puede darse el caso de que un satélite firme otros satélites no vistos por un usuario. Este caso no se considera explícitamente en la figura, suponiendo que, en condiciones de cielo abierto, se utilizan solamente satélites conectados por encima de una cierta elevación.

Esta situación se corresponde aproximadamente con lo que puede esperar un usuario cuando el mismo dispone de una vista sin obstrucciones del cielo después de que el sistema Galileo haya alcanzado su capacidad operativa completa. La suposición de que están conectados 2 de entre 8 satélites (es decir un 25%, o un promedio de 7,5 de entre 30) parece razonable puesto que actualmente se planifica el despliegue de 10 antenas de enlace ascendente. Cuantas más capacidades de enlace ascendente haya, menor será el tiempo entre autenticaciones (TBA) de los satélites y mejor será el rendimiento, hasta el caso en el que la mitad de los satélites estuviesen firmando a la otra mitad.

Con estas suposiciones, se obtienen los siguientes indicadores de rendimiento:

RENDIMIENTOS - AUTÓNOMO	
TTFA (nivel sat) [s]	36
TBA (nivel sat) [s]	24
TBA (nivel sat a Rx) [s]	12
Latencia de autenticación (nivel sat) [s]	32
TTFLLA [s]	48

El significado de estos indicadores de rendimiento viene dado por lo siguiente:

- "TTFA (nivel sat)" se refiere al transcurso de tiempo entre el inicio de la recepción de los datos a firmar desde un satélite específico, y el tiempo en el que están autenticados (4 s de recepción de datos + latencia de 8 s + transmisión de firma de 24 s = 36 segundos).
- "TBA (nivel sat)" se refiere al tiempo entre la recepción de dos firmas desde un satélite conectado específico. Puesto que se transmiten continuamente, "TBA (nivel sat)" es 24 segundos.
- "TBA (nivel sat a Rx)" se refiere al tiempo entre la recepción de firmas desde cualquier satélite conectado. Puesto que en el caso práctico hay 2 satélites conectados, y se supone que los mismos están sincronizados de manera óptima, "TBA (nivel sat a Rx)" es 24 / 2 = 12 segundos.

- “Latencia de autenticación” es el tiempo entre la recepción del último bit de la sección de mensaje a firmar y la recepción de la firma digital correspondiente (latencia de 8s + transmisión de 24 s = 32 segundos). Obsérvese que se supone que la latencia de autenticación para satélites conectados es 0.

- “TTFLLA”, o “Tiempo Hasta la Autenticación Completa”, se refiere al tiempo entre que el receptor comienza a procesar bits de navegación, y que el mismo puede calcular una posición usando 4 ó más satélites autenticados. Este no es un parámetro determinista aunque el valor de la tabla resulta plausible considerando las Figs. 5 y 6.

La Fig. 5 muestra un diagrama de temporización del tiempo hasta la autenticación en el nivel del receptor. Los bloques oscuros 100 representan las secciones de mensajes de navegación de satélites no conectados (satélites 1, 2, 4, 5, 7 y 8 en la Fig. 4, SV1, SV2, etcétera en las Figs. 5 y 6) a firmar por satélites conectados (satélites 3, 6 en la Fig. 4, SV3 y SV6 en las Figs. 5 y 6). Las flechas 102 enlazan las secciones de cada mensaje de navegación con el inicio de la transmisión de la firma digital DS correspondiente transmitida más tarde por otro satélite. Las celdas marcadas con un símbolo * o # implican que se ha autenticado un par de satélites (C y NC). Los números que aparecen en la parte inferior derecha del diagrama representan la latencia de autenticación (en segundos), es decir, el transcurso de tiempo entre la recepción de una sección de mensaje de navegación desde un primer satélite y la recepción de la firma digital correspondiente desde otro satélite.

TTFA en el nivel de satélite se produce después de 36 segundos, tras lo cual un usuario puede tener un punto de posición parcialmente autenticado (es decir, combinación de satélites autenticados y no autenticados). En el caso ilustrado, los primeros 4 satélites se autentican después de 48 segundos (= TTFLLA).

El diagrama de temporización de la Fig. 6 muestra la frecuencia y las latencias de autenticación observadas por los usuarios en la configuración de este ejemplo en modo estacionario. Si el usuario siempre toma los 4 satélites autenticados más recientemente, la “latencia de autenticación”, es decir, el transcurso de tiempo entre que se recibe una señal y que la misma se certifica como autentica, está entre 22 y 34 segundos. La “latencia de autenticación” del satélite autenticado más reciente está entre 0 segundos y 12 segundos. Esto significa que, siempre que una señal no haya sido suplantada cuando se autenticó por última vez, resultará muy difícil para un atacante suplantar una posición. Los números que aparecen en el diagrama de temporización en la parte central representan la latencia de autenticación, es decir, el transcurso de tiempo entre el final de la recepción de un segmento de mensaje de navegación y el final de la recepción de la firma digital correspondiente. Los números que aparecen en la parte inferior del diagrama representan la latencia de autenticación para los cuatro satélites con la latencia más baja, y el promedio de los mismos. El promedio pretende ser representativo de la latencia de autenticación total.

Los rendimientos obtenidos en términos de TTFA, TBA, TTFLLA y latencia parecen razonables para un receptor autónomo en una situación típica con buena visibilidad del cielo.

En la última parte de esta descripción, se describirán las amenazas que puede infringir un atacante al usuario, falseando las señales y/o la clave pública lo cual deriva en un punto de posición falso. Las amenazas se describen de una manera cualitativa.

La nomenclatura usada es:

- Pi: sección de mensaje de navegación de texto plano del satélite i que incluye la secuencia de bits aleatoria o seudoaleatoria,

- Pi’: mensaje de navegación de texto plano suplantado del satélite i,

- Hi: valor *hash* de Pi,

- Hi’: valor *hash* de Pi’,

- PRi: seudodistancia del satélite i,

- PRi’: seudodistancia suplantada del satélite i,

- Kpvi: Clave Privada para el satélite i (para generar firmar digital),

- Kpvi’: Clave Privada Falsa para el satélite i,

- Kpbi: Clave Pública para el satélite i (para descodificar la firma digital),

- Kpbi’: Clave Pública Falsa para el satélite i,

- DSi: Firma Digital para el mensaje de navegación del satélite i (sobre la base de Kpvi y Hi),

- DSi’: Firma Digital Suplantada para el mensaje de navegación del satélite i (sobre la base de Kpvi’ y Hi o Hi’)

Antes de analizar las amenazas, se recuerdan las siguientes propiedades de las firmas digitales:

- Un atacante no puede adivinar Kpvi conociendo Kpbi, Pi y DSi.
- Dado Hi, un atacante no puede generar DSi' de manera que Hi'(DSi', Kpbi) = Hi.

Estas son las etapas seguidas por el receptor para el proceso de autenticación:

1) Recepción y almacenamiento en el receptor de Kpbi (aproximadamente una vez por año).
2) Recepción de Pi a partir de la señal del satélite i.
3) Cálculo de PRi a partir de la señal del satélite i.
4) Cálculo de Hi a partir de Pi
5) Almacenamiento de Hi
6) Recepción de DSi del satélite j.
7) Cálculo de la posición sobre la base de Pi y PRi (de por lo menos cuatro satélites).
8) Verificación de Hi(DSi, Kpbi) con Hi(Pi) para los satélites usados en el cálculo de la posición (o un subconjunto de ellos)

La siguiente tabla presenta las amenazas potenciales de cada una de las etapas anteriores.

Etapas	**Amenazas**	**Viabilidad e Impacto**
1) Recepción y almacenamiento en el receptor de Kpbi	T1.1: Kpbi sustituido por Kpbi'	FI1.1: El receptor garantizará la autenticidad de Kpbi cuando se reciba (por ejemplo, una vez al año), y también protegerá contra la escritura del área de memoria en la que se almacene. Como clave pública, puede ser leída sin plantear ninguna amenaza de seguridad, pero no debería modificarse. Esta amenaza necesita combinarse con la suplantación de la señal para ser eficaz (T2.2).
2) Recepción de Pi a partir de la señal del satélite i.	T2.1: Pi se suplanta con Pi' T2.2: Pi se suplanta con Pi' & T1.1 T2.3: La parte de Pi que no se firma, se suplanta con Pi'.	FI2.1: Los bits impredecibles de Pi hacen que la suplantación resulte difícil. Si los bits impredecibles no son correctos, la comprobación de autenticación fallará cuando el receptor compare Hi'(Pi') con Hi(Kpbi, DSi'). FI2.2: Un suplantador puede A) falsear Kpbi con Kpbi' (T1.1), y B) Transmitir una señal suplantada Pi' con un valor *hash* Hi' y una firma DSi' sobre la base de una Kpvi' emparejada con Kpbi', de manera que Hi'(Kpbi', DSi') = Hi'(Pi') FI2.3: En presencia de un planteamiento de firma de mensajes de 4 segundos, el suplantador podría suplantar únicamente la parte de Pi que no se firma posteriormente. En este caso, el receptor perdería el enganche o se daría cuenta rápidamente de que o bien las seudodistancias no son coherentes o bien los parámetros de efemérides/relojes están cambiando continuamente, y plantearía una alerta de suplantación.

Etapas	Amenazas	Viabilidad e Impacto
3) Cálculo de PRi a partir de la señal del satélite i.	T3.1: PRi suplantada con PRi' T3.2 : El flujo continuo completo de la señal se reproduce/retransmite con señales falseadas.	FI3.1: Ataque SCER – Un suplantador puede reproducir los bits reales en tiempo real de una manera indetectable por un receptor, pero cambiando el ToA. Este tipo de ataque se considera más serio. Como el E1B I/NAV Galileo tiene una alta velocidad de símbolos (250 símbolos/s), es difícil materializar un ataque de este tipo. Para conseguir que el receptor sea robusto contra dichos ataques, puede que se requiera tomar algunas medidas en el nivel del receptor (como, por ejemplo, detector de J/N). FI3.2: la posición falseada se fijará en la antena del retransmisor de señales falseadas/repetidor. Si el retransmisor de señales falseadas está conectado al receptor, el ataque únicamente podría derivar en un error de temporización. Si el retransmisor de señales falseadas no está conectado al receptor, las mediciones de sensores de movimiento de bajo coste se podrían correlacionar con la PVT medida para identificar una discordancia y detectar un ataque.
4) Cálculo de Hi a partir de Pi	T4.1: Hi sustituido por Hi' en el receptor	FI4.1: Incluso si Hi se modifica a Hi', ningún Hi' puede conducir a una verificación correcta siempre que Kpbi sea correcta.
5) Almacenamiento de Hi	T5.1: Hi se modifica una vez que se ha recibido DSi	FI5.1: el receptor protegerá contra la escritura del área de memoria en la que está almacenado Hi.
6) Recepción de DSi del satélite j.	T6.1: DSi suplantada con DSi' T6.2: Kpvi es desentrañada por un suplantador. El suplantador genera DSi' coherente con Hi'.	FI6.1: Si Kbpi no ha sido falseada, un suplantador no puede falsear la señal de manera que Hi'(Pi') = Hi'(DSi', Kpbi); propiedades de las firmas digitales convencionales (véase más arriba) FI6.2: el sistema se diseñará de manera que Kpvi no se pueda desentrañar (usando un algoritmo de DS y una longitud de clave adecuados). Si Kpvi es desentrañada, se puede cambiar con el DSG. Requeriría una actualización de Kbi por parte de los usuarios.
7) Cálculo de la posición basándose en Pi y PRi (de por lo menos cuatro satélites)	T7.1: Pi o PRi almacenada en el receptor se sustituye por valores erróneos, o se falsea el proceso completo de cálculo de PVT.	FI7.1: El receptor protegerá el proceso de cálculo de PVT y/o notificará cuando este haya sido manipulado indebidamente.
8) Verificación de Hi(DSi, Kpbi) con Hi(Pi) para los satélites usados en el cálculo de la posición (o un subconjunto de los mismos)	T8.1: Se falsea el resultado de la comprobación de verificación.	FI8.1: El receptor protegerá el proceso de verificación y/o notificará cuando este haya sido manipulado indebidamente.

A partir del análisis (preliminar) de las amenazas, puede concluirse que el concepto propuesto de "autenticación cruzada de mensajes de navegación" (NMA Cruzada) no presenta debilidades adicionales en comparación con otros procesos de firma digital.

Aunque la NMA Cruzada está destinada principalmente a garantizar la autenticidad de los datos de navegación, introduce también un cierto nivel de robustez contra la suplantación del tiempo de llegada de las señales. Para obtener un aumento de la robustez, la NMA Cruzada se puede combinar con otras medidas anti-suplantación (por ejemplo, aquellas mencionadas anteriormente como estimación del reloj y detector de saltos, detector de interferencias deliberadas, u otras como sensores de navegación a estima, uso de varias antenas, monitorizadores de nivel de señal, etcétera).

El concepto se ha verificado con respecto a un conjunto de requisitos, que cubren las restricciones de implementación de los receptores, la viabilidad en el sistema Galileo, la retrocompatibilidad, la robustez y el rendimiento.

El concepto propuesto se podría implementar en receptores existentes de gran consumo, parece viable con la actual infraestructura aunque puede requerir algunas adaptaciones, es retrocompatible e introduce una robustez que se

considera que cumple las expectativas de los usuarios objeto de las señales de servicio abierto.

Aunque se han descrito de forma detallada realizaciones específicas, aquellos versados en la materia apreciarán que podrían desarrollarse diversas modificaciones y alternativas sobre esos detalles teniendo en cuenta las enseñanzas de conjunto de la exposición. Por consiguiente, los ejemplos, disposiciones y configuraciones particulares que se dan a conocer en la presente están destinados únicamente a ser ilustrativos, y no limitativos en cuanto al alcance de la invención, el cual viene dado por el ámbito completo de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para firmar digitalmente señales de radionavegación por satélite, que comprende

controlar un primer satélite de radionavegación de tal manera que dicho primer satélite introduce bits impredecibles en un primer mensaje de navegación difundido de manera general por dicho primer satélite, cuando dicho primer satélite no está enlazado en ese momento con un segmento de misión terrestre;

generar una firma digital de una sección de mensaje de navegación de dicho primer mensaje de navegación que contiene dichos bits impredecibles, mediante la aplicación de una función *hash* criptográfica sobre dicho mensaje de navegación según es recibido por un receptor monitorizador o una red de receptores monitorizadores y un cifrado subsiguiente;

transmitir dicha firma digital a un segundo satélite GNSS enlazado con dicho segmento de misión terrestre y

controlar dicho segundo satélite de tal manera que introduce dicha firma digital en un segundo mensaje de navegación difundido de forma general por dicho segundo satélite.

2. Método según la reivindicación 1, en el que dicho segundo satélite se controla además de tal manera que introduce un identificador en dicho segundo mensaje de navegación, de modo que dicho identificador identifica dicho primer mensaje de navegación como aquello que ha sido firmado digitalmente

3. Método según la reivindicación 1 ó 2, en el que dicha firma digital tiene una fortaleza equivalente de clave simétrica de por lo menos 112 bits.

4. Método según una cualquiera de las reivindicaciones 1 a 3, en el que dicha sección de mensaje de navegación que contiene dichos bits impredecibles y a la que se aplica la función *hash* y se firma, tiene una longitud en el intervalo de 400 a 500 bits.

5. Método según una cualquiera de las reivindicaciones 1 a 4, en el que dicha sección de mensaje de navegación que contiene dichos bits impredecibles y a la que se aplica la función *hash* y se firma, tiene una longitud de por lo menos 448 bits, en donde dicha función *hash* criptográfica es SHA-224 y dicho cifrado se basa en ECDSA K-233.

6. Método según una cualquiera de las reivindicaciones 1 a 5, en el que dichos primer y segundo mensajes de navegación son mensajes Galileo E1 I/NAV.

7. Método según una cualquiera de las reivindicaciones 1 a 6, en el que dicho primer satélite GNSS se controla de tal manera que introduce un primer preámbulo en dicho primer mensaje de navegación, precediendo a dichos bits impredecibles e identificando dichos bits impredecibles como tales.

8. Método según una cualquiera de las reivindicaciones 1 a 7, en el que dicho segundo satélite GNSS se controla de tal manera que introduce un segundo preámbulo en dicho segundo mensaje de navegación, precediendo a dicha firma digital e identificando dicha firma digital como tal.

9. Método según una cualquiera de las reivindicaciones 1 a 8, en el que dicho cifrado se lleva a cabo usando una clave privada de un par de claves criptográficas.

10. Método según una cualquiera de las reivindicaciones 1 a 9, que comprende recibir dicho mensaje de navegación que contiene dichos bits impredecibles en un receptor monitorizador o una red de receptores monitorizadores, y usar dicho mensaje de navegación recibido para generar dicha firma digital.

11. Método para autenticar señales de radionavegación por satélite, en el nivel del receptor de usuario, que comprende

recibir, en un receptor de usuario, una primera señal de radionavegación que es portadora de un primer mensaje de navegación difundido de manera general por un primer satélite de radionavegación que no está enlazado en ese momento con un segmento de misión terrestre, comprendiendo dicho primer mensaje de navegación una sección de mensaje de navegación que contiene bits impredecibles;

recibir, en dicho receptor de usuario, una segunda señal de radionavegación que es portadora de un segundo mensaje de navegación difundido de forma general por un segundo satélite de radionavegación enlazado en ese momento con un segmento de misión terrestre, conteniendo dicho segundo mensaje de navegación una firma digital, que se supone obtenida mediante la aplicación de una función *hash* criptográfica sobre dicha sección de mensaje de navegación según es recibida por un receptor monitorizador o una red de receptores monitorizadores, y un cifrado subsiguiente;

aplicar dicha función *hash* criptográfica sobre dicha sección de dicho primer mensaje de navegación que contiene dichos bits impredecibles para generar un valor *hash*;

descifrar dicha firma digital contenida en dicho segundo mensaje de navegación;

comparar dicho valor *hash* con dicha firma digital descifrada.

12. Método según la reivindicación 11, en el que dichas primera y segunda señales de radionavegación se consideran auténticas si dicho valor *hash* y dicha firma digital descifrada coinciden, si dicho receptor permanece enganchado a dicha primera señal de radionavegación durante la recepción de dicho primer mensaje de navegación y si dicho receptor permanece enganchado a dicha segunda señal de radionavegación durante la recepción de dicho segundo mensaje de navegación.

13. Método según la reivindicación 12, en el que se continúa considerando auténticas dichas primera y segunda señales de radionavegación mientras dicho receptor permanece enganchado a dichas primera y segunda señales de radionavegación, respectivamente.

14. Programa de ordenador ejecutable por un receptor de radionavegación por satélite, comprendiendo dicho programa de ordenador instrucciones que, cuando son ejecutadas por dicho receptor de radionavegación por satélite, consiguen que dicho receptor de radionavegación por satélite implemente el método de acuerdo con una cualquiera de las reivindicaciones 11 a 13.

15. Producto de programa de ordenador que comprende una memoria no volátil que tiene instrucciones almacenadas en la misma, las cuales, cuando son ejecutadas por un receptor de radionavegación por satélite, consiguen que dicho receptor de radionavegación por satélite implemente el método de acuerdo con una cualquiera de las reivindicaciones 11 a 13.

Fig. 1

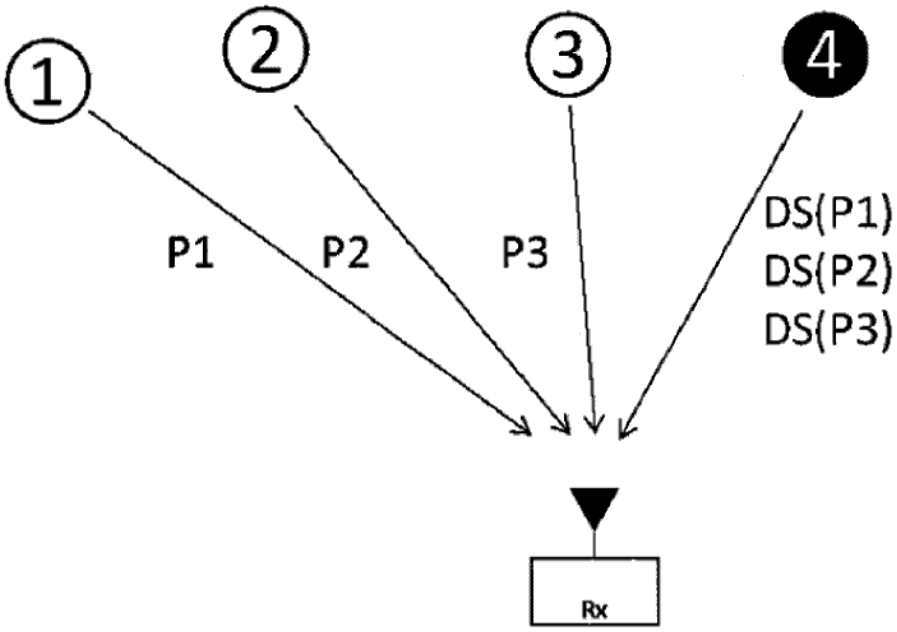
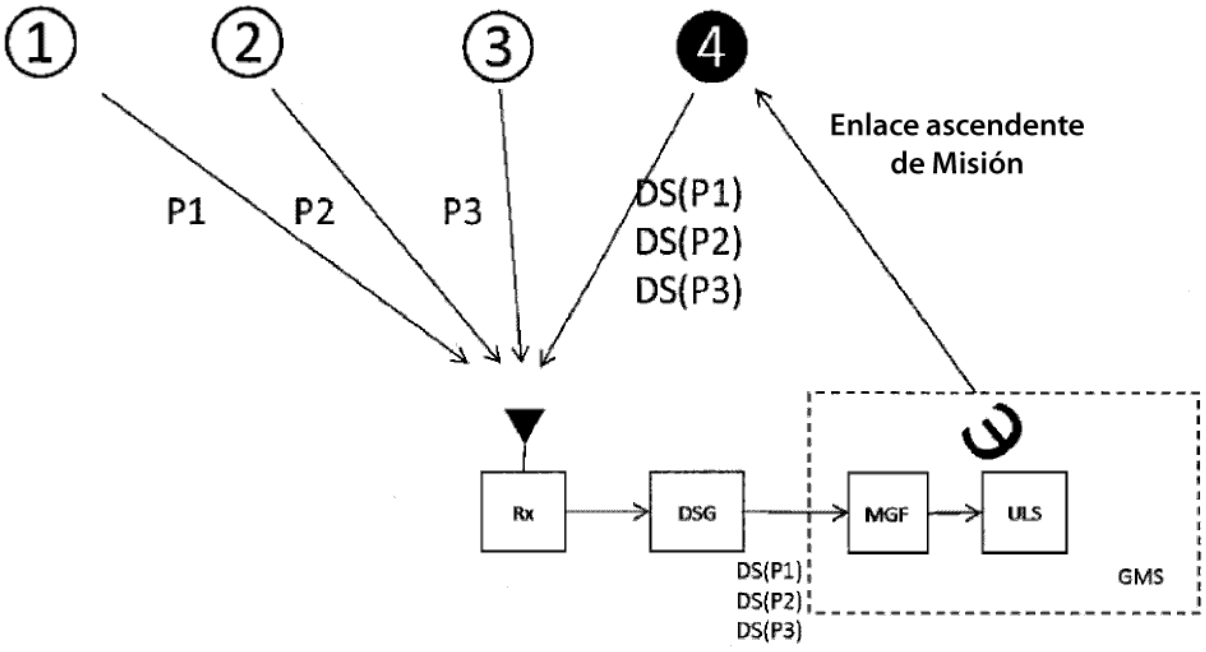

1
2
3
4
P1
P2
P3
DS(P1)
DS(P2)
DS(P3)
Rx

Fig. 2


1
2
3
4
P1
P2
P3
DS(P1)
DS(P2)
DS(P3)
Enlace ascendente de Misión
Rx
DSG
MGF
ULS
GMS
DS(P1)
DS(P2)
DS(P3)

SIN SATÉLITE CONECTADO

Campo "Reservado 1"		total [bits]
Preámbulo - NC	Bits aleatorios	
8	32	40

SATÉLITE CONECTADO - Durante sincronización con DSG

Campo "Reservado 1"		total [bits]
Preámbulo - S	Bits aleatorios	
8	32	40

SATÉLITE CONECTADO - Encabezamiento de DS

Campo "Reservado 1"			total [bits]
Preámbulo - C	ID Sat	DS	
8	6	12	40

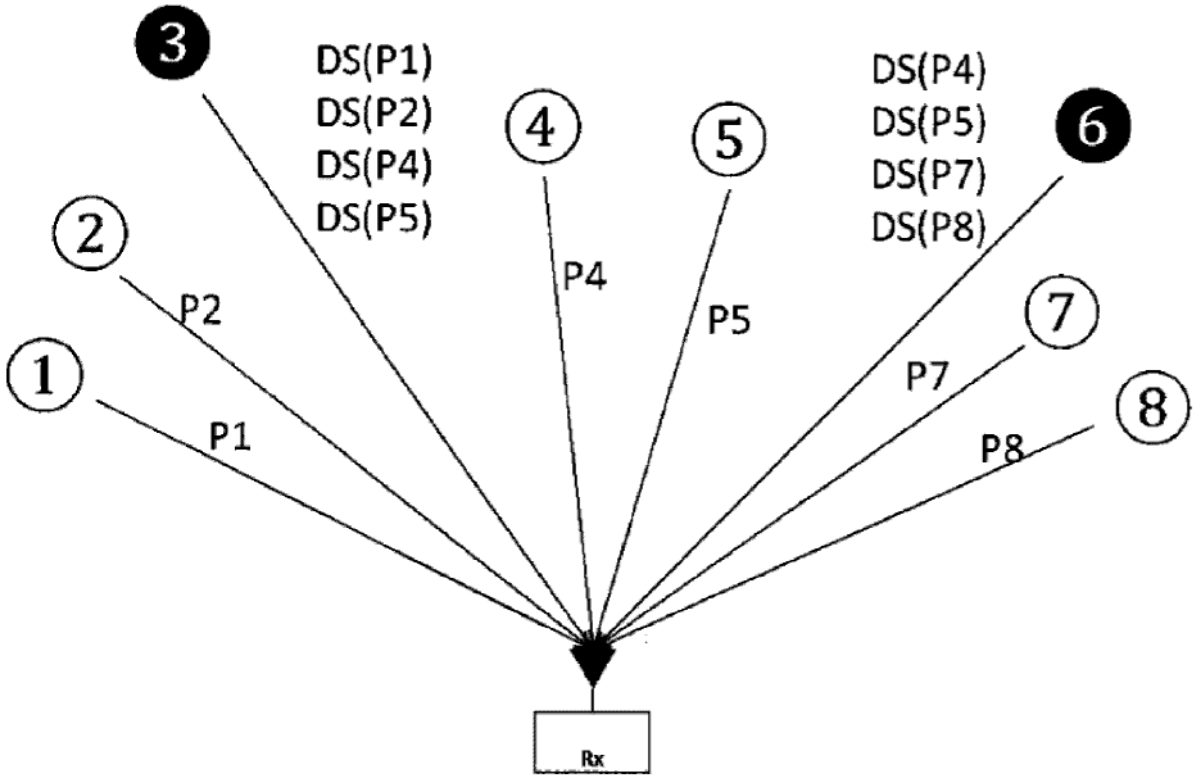
SATÉLITE CONECTADO - DS

Campo "Reservado 1"	total [bits]
Firma digital	
40	40

Generación a bordo	Generación en tierra

Fig. 3

Fig. 4


3
DS(P1)
DS(P2)
DS(P4)
DS(P5)
4
5
DS(P4)
DS(P5)
DS(P7)
DS(P8)
6
2
P2
P4
P5
7
1
P1
P7
8
P8
Rx

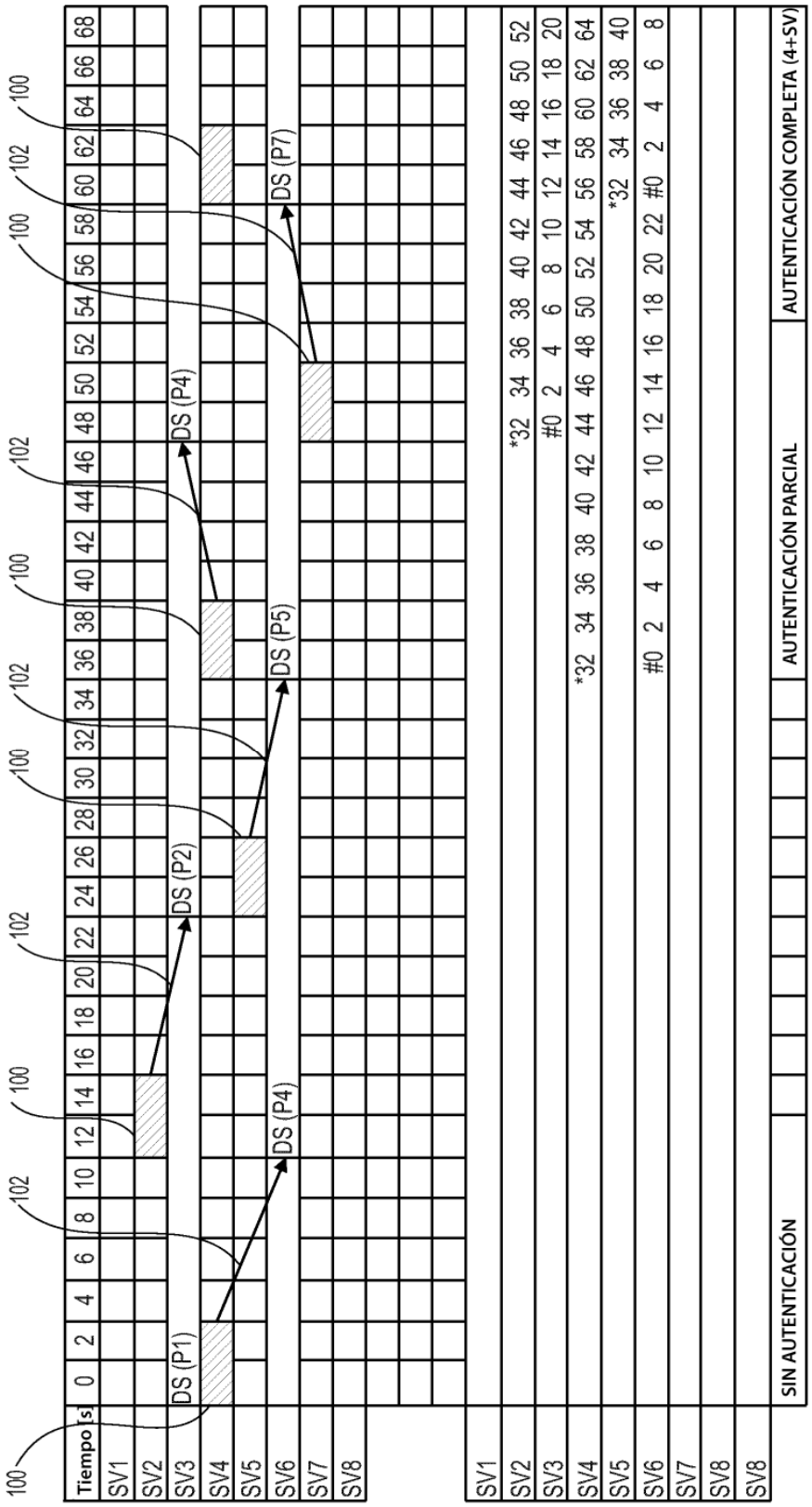

Tiempo [s]
SV1
SV2
SV3
SV4
SV5
SV6
SV7
SV8
DS (P1)
DS (P2)
DS (P4)
DS (P4)
DS (P5)
DS (P7)
SIN AUTENTICACIÓN
AUTENTICACIÓN PARCIAL
AUTENTICACIÓN COMPLETA (4+SV)

Fig. 5

Tiempo [s]	118	120	122	124	126	128	130	132	134	136	138	140	142	144	146	148	150	152	154	156	158	160	162	164	166	168	170	172
SV1																												
SV2																												
SV3		DS (P2)												DS (P4)												DS (P5)		
SV4																												
SV5																												
SV6	DS (P5)																			DS (P7)								
SV7																												
SV8																												
SV1		*32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80	82	84
SV2	102	104	106	108	110	112	114	116	118	120	122	124	126	*32	34	36	38	40	42	44	46	48	50	52	54	56	58	60
SV3	22	#0	2	4	6	8	10	12	14	16	18	20	22	#0	2	4	6	8	10	12	14	16	18	20	22	#0	2	4
SV4	78	80	82	84	86	88	90	*32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	*32	34	36
SV5	54	56	58	60	62	64	66	68	70	72	74	76	78	80	82	84	86	88	90	*32	34	36	38	40	42	44	46	48
SV6	10	12	14	16	18	20	22	#0	2	4	6	8	10	12	14	16	18	20	22	#0	2	4	6	8	10	12	14	16
SV7	66	68	70	72	74	76	78	80	82	84	86	88	90	92	94	96	98	100	102	104	106	108	110	112	114	116	118	120
SV8	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80	82	84	86	88	90	92	94	96
		MODO ESTACIONARIO (8SV)																										
ANTIGÜEDAD SAT MÁS RECIENTE [s]	10	0	2	4	6	8	10	0	2	4	6	8	10	0	2	4	6	8	10	0	2	4	6	8	10	0	2	4
2º SAT MÁS RECIENTE [s]	22	12	14	16	18	20	22	12	14	16	18	20	22	12	14	16	18	20	22	12	14	16	18	20	22	12	14	16
3er SAT MÁS RECIENTE [s]	42	32	34	36	38	40	42	32	34	36	38	40	42	32	34	36	38	40	42	32	34	36	38	40	42	32	34	36
4º SAT MÁS RECIENTE [s]	54	44	46	48	50	52	54	44	46	48	50	52	54	44	46	48	50	52	54	44	46	48	50	52	54	44	46	48
PROMEDIO 4 SATS MÁS RECIENTES [s]	32	22	24	26	28	30	32	22	24	26	28	30	32	22	24	26	28	30	32	22	24	26	28	30	32	22	24	26

Fig. 6