(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 478 876**

(51) Int. CI.:

G01S 19/02 (2010.01)
G01S 19/09 (2010.01)
H04W 12/10 (2009.01)
H04W 12/06 (2009.01)
H04W 12/12 (2009.01)
G01S 19/21 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.05.2011 E 11722807 (2)**

(97) Fecha y número de publicación de la concesión europea: **16.04.2014 EP 2583117**

(54) Título: **Procedimiento para proporcionar una indicación de tiempo-y-ubicación autenticable**

(30) Prioridad:

15.06.2010 EP 10166025

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.07.2014

(73) Titular/es:

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

(72) Inventor/es:

CHASSAGNE, OLIVIER

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Procedimiento para proporcionar una indicación de tiempo-y-ubicación autenticable.

Campo técnico

La presente invención se refiere en general a la autenticación de datos de posicionamiento. En particular, la invención se refiere a la provisión de una indicación de tiempo-y-ubicación autenticable, por ejemplo, en forma de un sello (*stamp*) digital de tiempo-y-ubicación, incorporado a un documento u otros datos, usando un receptor de señales de radionavegación. Otro aspecto de la invención se refiere a la autenticación de los datos de posicionamiento, es decir, el proceso de decidir si una supuesta indicación de tiempo-y-ubicación es o no auténtica.

Antecedentes de la técnica

La radionavegación, en particular la navegación por satélite, segura, será el día de mañana tan importante y vital como lo es hoy en día la segura red de Internet. Sin embargo, muchas de las amenazas sobre la navegación por satélite no se pueden evitar o combatir a través de las tecnologías actuales por lo menos para aplicaciones civiles para el público general.

Hay varias aplicaciones de posicionamiento, en las cuales es necesario conocer con un alto grado de certeza y fiabilidad la verdadera posición de un usuario en un determinado momento. Dichas aplicaciones incluyen, por ejemplo, la gestión de flotas, peajes en carreteras, geo-delimitación, licencias de sitios virtuales, servicios basados en la ubicación críticos en cuanto a la seguridad, planes de seguro del coche del tipo pago-como-conduzco, etcétera. En otras aplicaciones, puede que sea necesario establecer si un usuario se encontraba en posesión de ciertos datos en un momento y una ubicación determinados.

La penetración en el mercado y la aceptación, por parte de los usuarios, de estas aplicaciones dependerá en gran medida de su fiabilidad y de la confianza en la integridad y robustez de los servicios que se prestan. En este contexto, los usuarios de la invención abarcan tanto usuarios de receptores, cuyas posiciones se determinan basándose en señales de radionavegación del sistema de radionavegación (típicamente, a estos usuarios se les hace referencia como “usuarios finales”), como proveedores de servicios, que usan los datos de posicionamiento recibidos de los usuarios finales. A estos proveedores de servicios se les puede hacer referencia como proveedores de servicios externos ya que normalmente son distintos del operador del sistema de posicionamiento.

Por una parte, los usuarios finales típicamente desean tener seguridad de la autenticidad de la fuente de las señales de radionavegación. Esta preocupación está vinculada con el concepto al que, en lo sucesivo en la presente, se hará referencia como autenticación de señal-en-el-espacio (SIS).

Por otra parte, los proveedores de servicios externos típicamente desean tener la garantía de que cada uno de los datos de posicionamiento que reciben de sus usuarios finales (abonados) se corresponde realmente con la posición del usuario final en el momento indicado. Esto implica, en primer lugar, que los datos de posicionamiento se han calculado sobre la base de señales de radionavegación auténticas y, en segundo lugar, que no han sido manipulados indebidamente, es decir, modificados o falsificados con el fin de proporcionar una posición o tiempo erróneos.

Al concepto referente a la autenticación de los datos de posicionamiento declarados por usuarios finales o transmitidos por sus receptores de señales de radionavegación se le hará referencia en lo sucesivo en la presente memoria como autenticación de posición-velocidad-tiempo (PVT). PVT significa posición-velocidad-tiempo, el conjunto más común de datos de posicionamiento calculados por los receptores.

La solicitud de patente internacional WO 2009/090515 hace frente al problema de la autenticación de datos de posicionamiento en el contexto de los peajes de carretera sin infraestructuras. El sistema de tarificación en un sistema automatizado de peajes en carretera se basa en la distancia recorrida, la fecha y/u hora del traslado, la ubicación (área geográfica) y/o las características del vehículo (longitud, capacidad cúbica, consumo de combustible, emisiones de CO_2, etcétera). El documento WO 2009/090515 pretende evitar el denominado “ataque de GPS ficticio”, es decir, la provisión de datos falsos de GPS a la organización encargada del peaje para reducir la cantidad a pagar por el peaje de carretera. Esto se materializa proporcionando, a la organización encargada del peaje, lecturas de sensores del estado del vehículo (velocidad, ángulo de dirección, distancia del viaje, tiempo local, etcétera). A continuación la organización encargada del peaje coteja los datos GPS con los datos del estado del vehículo con el fin de autenticar o invalidar los datos GPS.

La solicitud de patente internacional WO 2009/001294 también se refiere a la prevención y detección de fraudes en el contexto de un sistema de peajes en carretera. El receptor de usuario recupera los datos de posicionamiento mediante la recepción, conversión en sentido descendente y procesado de señales de navegación. A la organización encargada del peaje se le proporcionan a continuación los datos de posición decodificados así como datos sin procesar (muestras de las señales de navegación convertidas en sentido descendente), y puede comprobar

entonces si la muestra de datos sin procesar se corresponde con lo esperado en la ubicación y el tiempo particulares indicados por la información de posición transmitida.

La patente US nº 5.754.657 sigue un planteamiento similar, dando a conocer un procedimiento de autenticación o validación en el que el receptor cuya posición va a ser validada o invalidada transmite una "señal de datos aumentada" que comprende datos de señales de radionavegación sin procesar así como la posición y el tiempo aseverados. La "señal de datos aumentada" se transmite a una estación central, la cual esencialmente comprueba si los datos sin procesar son congruentes con la posición y tiempo aseverados así como con las señales difundidas por los satélites.

En el artículo "Signal Authentication - A Secure Civil GNSS for Today", de Sherman Lo et al., publicado en la edición de septiembre/octubre de 2009 de InsideGNSS se propone otra solución interesante. El procedimiento de autenticación dado a conocer en este artículo se basa en el hecho de que la frecuencia GPS L1 transporta señales tanto de código C/A como de código P(Y) (cifradas), transmitidas en cuadratura de fase. El receptor de usuario transmite su posición y tiempo calculados junto con una instantánea de las señales de código P(Y) (sin procesar) a una autoridad de autenticación. El procedimiento saca provecho de que la secuencia de código P(Y) recibida en una primera ubicación (la ubicación de un receptor, cuya posición va a ser autenticada) es idéntica a la secuencia de código P(Y) recibida en una segunda ubicación (la ubicación de un receptor de referencia bajo el control de la autoridad de autenticación), si se tiene en cuenta la diferencia de los tiempos de las señales del receptor-al-satélite. La presencia de un pico de correlación en las secuencias de código P(Y) (sin procesar) registradas en las dos ubicaciones establece una autenticidad de señal del código C/A (si se supone que ambos receptores no se encuentran simultáneamente dentro del alcance de recepción del mismo atacante de suplantación de identidad de señales). Aspectos del procedimiento dado a conocer en el artículo también han sido objeto de las solicitudes de patente US 2009/0195443 y US 2009/0195354.

Básicamente, existen tres tipos diferentes de amenazas a la integridad de datos de posicionamiento:

- Amenazas a la integridad de las señales-en-el-espacio (por ejemplo, interferencias deliberadas, suplantación de identidad y retransmisión de señales falseadas (*meaconing*)). Estas son amenazas que se producen "aguas arriba" del cálculo de los datos de posicionamiento. Las interferencias deliberadas son la emisión de una señal o ruido de radiofrecuencia con potencia suficiente y con características específicas con el fin de suplantar las señales de navegación en las proximidades del emisor de señales interferentes deliberadas. Las interferencias deliberadas tienen el efecto de evitar que receptores de posicionamiento adquieran y realicen un seguimiento de señales de navegación dentro de un área, cuya superficie depende de la potencia de emisión del emisor de señales interferentes deliberadas. El receptor de posicionamiento sometido a un ataque de interferencias deliberadas se vuelve incapaz de producir datos de PVT o solamente puede producir datos de PVT afectados por una alta incertidumbre (que presentan un intervalo grande de errores). Todas las señales, cifradas o no, pueden ser objeto de interferencias deliberadas. Los emisores de señales interferentes deliberadas están disponibles en el mercado a precios bajos (menos de 100€). Las interferencias deliberadas pueden detectarse por medio de receptores de posicionamiento equipados con dispositivos y algoritmos ad hoc. Las interferencias deliberadas son una actividad ilegal en la mayoría de los países. La suplantación de identidad es la difusión general de señales que se asemejan a señales de posicionamiento por parte de un simulador situado en tierra con el fin de engañar a receptores de posicionamiento. La suplantación de identidad es ilegal en la mayoría de los países. Los dispositivos para suplantación de identidad no pueden simular en principio señales cifradas (por ejemplo, el código P(Y) GPS actual, el futuro código M GPS, o los futuros códigos PRS y CS del Galileo) a no ser que puedan desentrañar el cifrado del código de navegación, lo cual es muy poco probable. Los dispositivos para suplantación de identidad no se encuentran fácilmente disponibles en el mercado todavía pero pueden ser producidos de manera sencilla por fabricantes de receptores y/o por personas versadas en la técnica. Se espera que en unos años habrá disponibles en el mercado dispositivos para suplantación de identidad a precios asequibles entre aproximadamente 100 € y 1.000 €. La retransmisión de señales falseadas es la recepción y re-difusión general de señales de navegación genuinas, con o sin un retardo de tiempo. Las señales originales se leen usando una antena de alta calidad, se retardan y a continuación son retransmitidas por un emisor, de manera que las señales retardadas conduzcan al cálculo de una posición errónea. A diferencia de la suplantación de identidad, la retransmisión de señales falseadas puede, bajo ciertas condiciones, engañar también a receptores de posicionamiento que trabajan con señales de navegación cifradas.

- Amenazas al cálculo de la PVT (por ejemplo, errores de programación, gusanos informáticos y/o virus de hardware o software que alteran el proceso de cálculo).

- Amenazas a la integridad de la PVT después de su cálculo (manipulación indebida de la PVT calculada) o después de su supuesto cálculo (en el caso de datos de posicionamiento completamente inventados). Una PVT podría, por ejemplo, ser interceptada y sustituida por una PVT ficticia en la transmisión a través de redes de telecomunicaciones entre el receptor de usuario y el proveedor de servicios externo. La misma también podría modificarse cuando se almacena en soportes electrónicos, por ejemplo, dentro de las instalaciones del proveedor de servicios.

Problema técnico

Existen dos conceptos principales de autenticación que se producen en el contexto de la radionavegación. Al primero se le hace referencia en lo sucesivo en la presente memoria como “autenticación de SIS autónoma”, donde “SIS” es el acrónimo de señal-en-el-espacio, es decir, la señal que llega al receptor. La autenticación de SIS autónoma permite a un usuario de un receptor GNSS, o al propio receptor, verificar que las señales utilizadas para calcular una posición son las correspondientes de una constelación GNSS dada (y no señales difundidas por un dispositivo aéreo o basado en tierra malintencionado) y que se ha calculado mediante un algoritmo fiable. La autenticación de SIS autónoma pretende así autenticar las fuentes de señales de radionavegación. La autenticación de SIS autónoma hace frente a las dos siguientes preguntas, en las cuales está interesado todo usuario del receptor GNSS:

- ¿Se está sometiendo al receptor a una suplantación de identidad?
- ¿Es fiable el software del receptor?

Al segundo concepto de autenticación se le hace referencia, en lo sucesivo en la presente memoria, como autenticación de PVT remota. Sirve para terceros que desean comprobar las posiciones declaradas por usuarios. La autenticación de PVT remota permite a un tercero validar que datos de posicionamiento producidos por un receptor de radionavegación, tenga o no otros sensores integrados, no han sido manipulados indebidamente, es decir, no se han modificado o falsificado con la finalidad de proporcionar, por ejemplo, una posición errónea, una velocidad errónea y/o un tiempo erróneo. El concepto de autenticación de PVT remota evalúa el grado de fiabilidad de datos de posicionamiento ya registrados y de la fuente que ha producido estos datos de posicionamiento.

La autenticación de PVT remota va dirigida a las siguientes preguntas en las cuales está interesado un receptor de datos de posicionamiento:

- ¿Se puede confiar en estos datos de posicionamiento?
- ¿Proceden los datos de posicionamiento del receptor del cual se afirma que los ha producido?

La autenticación de la posición de extremo-a-extremo es la conjunción, o la combinación, tanto de la autenticación de SIS autónoma como de la autenticación de PVT remota dentro de una sola aplicación. Es exactamente a lo que aspira el presente ejemplo.

Merece la pena poner énfasis nuevamente en el motivo por que se hace distinción entre autenticación de SIS autónoma y autenticación de PVT remota.

La autenticación de SIS autónoma garantiza que las señales leídas por un receptor de radionavegación son las correspondientes difundidas por una constelación GNSS - o una constelación de pseudolites - y no las difundidas por un dispositivo malintencionado. La autenticación de SIS autónoma concierne principalmente al usuario final. En otros términos, la autenticación de SIS autónoma es lo que desean los usuarios de receptores GNSS. Responde a la pregunta de si el usuario de un receptor GNSS puede fiarse del posicionamiento proporcionado por su receptor. La autenticación de PVT remota garantiza que los datos de posicionamiento no han sido manipulados indebidamente desde el mismo momento en el que dichos datos de posicionamiento fueron calculados. La autenticación de PVT remota concierne a terceros que se encuentran en una relación contractual con usuarios de los receptores de radionavegación o que tienen una autoridad de control sobre usuarios. No concierne al usuario del receptor de radionavegación. En otros términos, la autenticación de PVT remota es lo que desean los terceros. Responde a la pregunta de si un tercero puede confiar en los datos de posicionamiento enviados por un usuario.

Adicionalmente, la autenticación de SIS autónoma se podría usar para proporcionar al usuario información sobre el nivel de confianza vinculado a la precisión del posicionamiento, especialmente en situaciones en las que efectos locales, tales como multi-trayectos, están perturbando mediciones de SIS.

Cabe señalar que la autenticación de SIS autónoma sola no tiene ningún valor para terceros que buscan datos de posicionamiento de confianza, ya que los datos de posicionamiento proporcionados a los terceros podrían haber sido falsificados. Adicionalmente, la autenticación de SIS remota sola resulta menos interesante sin la autenticación de SIS autónoma: si la autenticidad de las señales utilizadas para calcular los datos de posicionamiento no se puede comprobar, los datos de posicionamiento se podrían haber calculado sobre la base de señales de radionavegación cuya identidad se ha suplantado. Incluso en ausencia de cualquier modificación de los datos de posicionamiento, no se pueden confiar plenamente en ellos.

Se puede señalar además que se considera más sencillo confiar en una “autoridad de confianza” que en dos autoridades. En otras palabras, aunque en teoría es concebible tener dos entidades diferentes, una primera que proporcione autenticación de SIS autónoma y una segunda que proporcione autenticación de PVT remota, en la práctica sin embargo, la coexistencia de dos entidades independientes hará que los procedimientos resulten bastante más complejos por la siguiente razón: ambas dependen del mismo receptor de radionavegación y de su

naturaleza a prueba de manipulaciones indebidas. Además, si dos entidades diferentes fueran a proporcionar la autenticación de SIS autónoma y la autenticación de PVT remota, respectivamente, el receptor seguiría siendo el eslabón débil de la cadena de confianza. En tal caso, siempre existe un riesgo de un ataque del tipo hombre-en-el-medio en la interfaz, es decir, dentro del receptor. Por ejemplo, personas dispuestas a engañar podrían colocar un simulador de PVT entre las dos aplicaciones. Un ataque de este tipo es imposible en la aplicación que se describe posteriormente en la presente.

Es un objetivo de la presente invención proporcionar un procedimiento para calcular datos de posicionamiento autenticables, es decir, datos de posicionamiento cuya autenticidad se puede verificar posteriormente por parte de una autoridad de autenticación. Este objetivo se logra con un procedimiento según la reivindicación 1.

Descripción general de la invención

La presente invención se puede implementar en el contexto de cualquier tipo de Sistema de Navegación Global por Satélite (GNSS) o un sistema de radionavegación que use una constelación de pseudolites. Un aspecto clave de la invención es que las fuentes de señales de radionavegación (satélites o pseudolites) difunden señales de radionavegación que contienen un testigo criptográfico dentro de su contenido de datos. Los testigos (*tokens*) criptográficos se pueden considerar como números pseudo-aleatorios o claves (por ejemplo, en forma de una secuencia binaria) que se actualizan de vez en cuando bajo el control de una autoridad de autenticación. Son impredecibles en el sentido de que, en términos de probabilidades, es imposible obtener futuros testigos criptográficos a partir del historial de los testigos criptográficos, es decir, algunos o la totalidad de los difundidos previamente. En este sentido, los testigos criptográficos pueden considerarse como *nonces* (del inglés “numbers used once” – “números usados una vez”) criptográficos – aun cuando un valor específico del testigo criptográfico pueda repetirse (en momentos impredecibles).

Los testigos criptográficos son usados como variable criptográfica por receptores de señales de radionavegación dedicados, para añadir un sello digital y/o cifrar la solución de posicionamiento calculada, es decir, la posición geográfica y el tiempo calculados sobre la base de las señales de radionavegación recibidas. Los receptores producen a continuación un paquete de datos que comprende una primera y una segunda partes, incluyendo la primera de ellas los datos de posicionamiento (la solución de posicionamiento) y un identificador público de receptor, y conteniendo la segunda parte un resumen (*digest*) (valor *hash*) o un encapsulamiento (cifrado) de la solución de posicionamiento. Los paquetes de datos pueden almacenarse en el receptor y/o se pueden comunicar a otras entidades, por ejemplo, un proveedor de servicios externo.

En el presente contexto, la expresión “datos de posicionamiento” se interpreta de manera que comprende tiempo y posición geográfica (en 2D, por ejemplo, como longitud y latitud, o en 3D, por ejemplo, como longitud, latitud y altitud), posiblemente en combinación con uno o más de los siguientes tipos de datos:

- velocidad (vector);
- aceleración (vector);
- sobreaceleración (vector), es decir, (vector del) ritmo de variación de la aceleración;
- rumbo (vector),
- datos de precisión e integridad tal como las dimensiones de una caja de confianza centrada en el tiempo y la posición geográfica calculados, que indica qué fracción de espacio-tiempo contiene el tiempo y la posición geográfica reales con una probabilidad dada (nivel de confianza).

A continuación se pueden presentar paquetes de datos a la autoridad de autenticación, que comprueba si el tiempo y la posición geográfica indicados en el paquete de datos son congruentes con el resumen y/o el texto cifrado. Con este fin, la autoridad de autenticación mantiene un archivo de los testigos criptográficos que se han difundido o usa un algoritmo para recuperar los testigos criptográficos correspondientes a la posición y tiempo aseverados. En función del resultado de la comprobación de congruencia, la autoridad de autenticación puede establecer a continuación un certificado que exponga la autenticidad del paquete de datos o que indique que la comprobación de congruencia ha fallado. Si la comprobación de congruencia falla, cabe suponer con mucha veracidad que el paquete de datos ha sido manipulado indebidamente o que se ha generado bajo condiciones irregulares (por ejemplo, bajo un ataque de interferencias deliberadas, de suplantación de identidad o de retransmisión de señales falseadas).

Si los testigos criptográficos pudieran extraerse fácilmente del mensaje de datos de las señales de radionavegación, sería teóricamente viable, para un tercero malintencionado, archivar los testigos criptográficos difundidos y usar estos testigos archivados para falsificar, dados una posición geográfica y un tiempo determinados, un resumen y/o un texto cifrado adecuados, y ensamblar un paquete de datos en el formato correcto. En ausencia de medidas de seguridad adicionales, el paquete de datos falsificado sería entonces posiblemente considerado como auténtico por la autoridad de autenticación.

Existen varias opciones para conseguir que este tipo de ataque resulte extremadamente difícil. Para denegar acceso a los testigos criptográficos, los mismos se protegen mediante cifrado cuando se difunden en las señales de radionavegación. Con este fin, los testigos criptográficos pueden distribuirse sobre señales de radionavegación seguras. Una señal de radionavegación se califica como segura si se cumple una de las siguientes condiciones:

(a) la señal de radionavegación está en sí misma cifrada (es decir, el código de determinación de la distancia (*ranging code*) de la señal está cifrado) con un algoritmo de cifrado del estado de la técnica, o

(b) la señal de radionavegación no está cifrada (señal abierta) pero el mensaje de datos (incluyendo los testigos criptográficos) que transporta está cifrado con un algoritmo de cifrado del estado de la técnica; o

(c) tanto la señal de radionavegación como su mensaje de datos están cifrados con el mismo algoritmo de cifrado del estado de la técnica o dos algoritmos de cifrado diferentes, con dos series de claves diferentes.

Los testigos criptográficos pueden ser comunes a algunas o la totalidad de las fuentes de señales de radionavegación, es decir, estas fuentes de señales difunden así la misma secuencia cronológica de testigos criptográficos. Alternativamente, cada fuente de señales de radionavegación se puede caracterizar por un testigo criptográfico específico. En esta opción alternativa, cada fuente de señales de radionavegación difunde su propia secuencia cronológica de testigos criptográficos, siendo dichas secuencias de testigos mutuamente distintas entre las diversas fuentes de señales. En esta opción, el receptor de señales de radionavegación recibe una pluralidad de testigos criptográficos para cada punto (*fix*) de posición. La variable criptográfica usada para añadir un sello digital y/o cifrar la solución de posicionamiento calculada es por lo tanto una función de la pluralidad de testigos criptográficos. En este escenario, la variable criptográfica depende del tiempo del punto de posición (en la medida en la que los testigos criptográficos se actualizan regularmente) y de la posición geográfica (en la medida en que las fuentes de señales de radionavegación bajo visibilidad del receptor dependen de su ubicación actual). Se observará que, incluso en caso de que cada fuente de radionavegación difunda su secuencia de testigos individual, puede haber momentos en los cuales algunos de los testigos recibidos de fuentes diferentes tengan accidentalmente el mismo valor.

Como aspecto de seguridad adicional, el acceso a los testigos criptográficos se realiza preferentemente condicionado al uso de un tipo predeterminado de hardware (por ejemplo, un módulo criptográfico) y/o software del receptor, en particular un hardware y/o software del receptor a prueba de manipulaciones indebidas. El receptor comprende así ventajosamente un perímetro de seguridad para ejecutar todas las operaciones críticas en cuanto a seguridad y para evitar que cualquier tercero lea los testigos criptográficos. Una huella digital del software del receptor se puede incluir en el paquete de datos para permitir que la autoridad de autenticación compruebe que el software del receptor no ha sido alterado. Si se proporciona al mismo una huella digital no válida, la autoridad de autenticación emitirá un certificado que alerte sobre la alteración del software.

Preferentemente, las claves que conceden a los receptores acceso a las señales de radionavegación (cifradas) y/o los testigos criptográficos (preferentemente junto con el mensaje de navegación) se distribuyen solamente a receptores que superan una verificación de su software y/o hardware, de acuerdo con un protocolo de comunicaciones seguro. Las claves para acceder a los testigos criptográficos y/o la clave para acceder a las señales de radionavegación preferentemente se cambian de vez en cuando para garantizar que receptores cuyo perímetro de seguridad ha sido manipulado indebidamente no tengan acceso a largo plazo a los testigos criptográficos. Esto hace que a un atacante que usa receptores pirateados le resulte considerablemente más difícil construir un archivo exhaustivo de los testigos criptográficos pasados. En la práctica, en casos en los que las claves se actualizan, cuando está a punto de producirse la expiración de las claves que conceden acceso a las señales de radionavegación y/o los testigos criptográficos, almacenadas en el receptor, este último puede establecer un canal de comunicaciones seguro con la autoridad de autenticación de forma automática o puede invitar al usuario a hacerlo con el fin de recuperar las claves posteriores.

Mientras que las firmas digitales convencionales se ocupan de la autenticación del autor o de la fuente de un mensaje o un documento digital, la invención no autentica al usuario del receptor per se, sino que puede ampliar el alcance de las firmas digitales con información segura sobre cuándo y dónde se ha producido una firma digital, siempre que el dispositivo de firma esté configurado de acuerdo con la presente invención.

Varios segmentos del sistema de radionavegación tienen relación con la presente invención, tales como:

- el segmento terrestre del sistema de radionavegación, que se encuentra a cargo de, entre otros aspectos, la sincronización de los satélites y/o pseudolites y la preparación del mensaje de datos para ser difundido sobre las señales de radionavegación;

- el segmento de las fuentes de señales de radionavegación (satélites y/o pseudolites); en el caso de un sistema global de navegación por satélite, a esto se le hace referencia como “segmento espacial”, que comprende típicamente de manera aproximada entre 24 y 30 satélites operativos en una órbita terrestre

media sobre tres o seis planos orbitales diferentes;

- el segmento de usuario que comprende los receptores de radionavegación;
- la autoridad de autenticación, o la autoridad de autenticación;
- cuando sea aplicable, un segmento de telecomunicaciones para la transmisión de paquetes de datos desde receptores a proveedores de servicios geo-localizados ("red por paquetes de datos"); y
- un segmento de telecomunicaciones seguro para la distribución de las claves que dan acceso a las señales de radionavegación y/o los testigos criptográficos para los receptores.

El solicitante se reserva el derecho de dirigir reivindicaciones a los diferentes aspectos de la invención por separado, posiblemente en una o más aplicaciones divisionales o de continuación cuando así resulte apropiado.

Volviendo en primer lugar al segmento de usuario, un aspecto de invención trata sobre un procedimiento para proporcionar datos de tiempo-y-ubicación autenticables usando un receptor de señales de radionavegación. El procedimiento comprende recibir señales de radionavegación difundidas desde una pluralidad de fuentes de señales de radionavegación (por ejemplo, satélites o pseudolites), conteniendo por lo menos algunas de estas señales de radionavegación, en sus mensajes de datos, uno o más testigos criptográficos protegidos mediante cifrado y actualizados de vez en cuando, preferentemente bajo el control de una autoridad de autenticación. El receptor recupera, mediante descifrado, los testigos criptográficos a partir de las señales de radionavegación. Si las señales de radionavegación que transportan los testigos están cifradas, el receptor obtiene acceso a los mensajes de datos de las señales usando la clave correspondiente. De modo similar, si los propios testigos criptográficos están cifrados (sobre una señal abierta o cifrada), el receptor los descifra usando la clave apropiada. A continuación el receptor determina datos de posicionamiento, incluyendo su posición geográfica y tiempo (fecha y hora del día), sobre la base de las señales de radionavegación recibidas, es decir, materializa un punto de posición y determina el tiempo. El receptor genera un código de autenticación digital, el cual es un resumen del mensaje criptográfico, o un texto cifrado o una combinación de un resumen y un texto cifrado, por medio de una función criptográfica que toma como entradas por lo menos los datos de posicionamiento y los testigos criptográficos recuperados. El receptor produce a continuación un paquete de datos que incluye una primera parte que contiene los datos de posicionamiento mencionados anteriormente, un identificador público de receptor (es decir, un marcador escrito en el receptor) y una segunda parte que contiene el código de autenticación digital mencionado anteriormente. Los propios testigos criptográficos se usan para producir el código de autenticación digital aunque no se incluyen en el paquete de datos.

Todavía dentro del segmento de usuario, otro aspecto de la invención trata sobre un receptor de señales de radionavegación configurado para llevar a cabo este procedimiento. Con este fin, el receptor está equipado con hardware y software adecuados. Un aspecto de la invención trata así sobre un programa de ordenador para un receptor de señales de radionavegación, que comprende instrucciones que, cuando son ejecutadas por el receptor de señales de radionavegación, consiguen que el mismo funcione de acuerdo con el procedimiento.

La función criptográfica puede por ejemplo, producir, en calidad de código de autenticación digital, un resumen digital en forma de un valor *hash* de los datos de posicionamiento y posiblemente el identificador público de receptor, usando, en calidad de variable criptográfica, una clave criptográfica que es una función (por ejemplo, una concatenación) de por lo menos los testigos criptográficos recuperados. Alternativa o adicionalmente, la función criptográfica puede cifrar los datos de posicionamiento y posiblemente el identificador público de receptor usando dicha clave criptográfica como variable criptográfica.

Se observará que, además de los datos de posicionamiento y del identificador público del receptor, la función criptográfica puede tomar como entradas datos adicionales a proteger, por ejemplo, uno o más documentos digitales, tales como fotografías digitales, datos de identificación de usuarios, datos de integridad de señales-en-el-espacio, una huella digital de software del receptor, datos de posicionamiento complementarios, firmas digitales, etcétera. El código de autenticación digital en este caso sirve para establecer que estos datos adicionales fueron almacenados o gestionados por el receptor en un cierto tiempo y en una cierta ubicación.

La invención por lo tanto se puede usar para proteger no solamente

- la identificación del receptor y los datos de posicionamiento que el mismo produjo, sino también, de forma adicional, otra información que identifica al usuario o referente al mismo; y/o
- cualquier documento digital procesado por el receptor, tal como fotografías, películas; documentos escaneados, archivos de datos de las mediciones.

Ventajosamente, los datos adicionales a proteger pueden incluir:

- Datos de identificación que identifican al usuario del receptor y/o cualquier forma digital de autorizaciones

administrativas propiedad del usuario (tales como un permiso de conducción, una licencia de piloto, un certificado de registro del coche, un certificado del seguro del coche, derechos digitales para acceder a documentos multimedia); incluyendo una huella digital del código de programa del software del receptor; y/o

- datos de alerta por ataques; y/o
- cualquier dato o documento digital producido por un dispositivo tal como un dispositivo de medición, una máquina fotocopiadora, una cámara fotográfica, una grabadora de video, etcétera, equipado con un receptor de señales de radionavegación incorporado.

Para simplificar, a los datos de posicionamiento y a los datos adicionales opcionales a proteger se les puede hacer referencia, en lo sucesivo en la presente memoria, simplemente como “datos a proteger”.

Existen varias maneras en las cuales se puede configurar la función criptográfica para proteger los datos que recibe como entradas. Por ejemplo, la función criptográfica podría producir un valor *hash* (resumen) de algunos o la totalidad de los datos a proteger usando la clave criptográfica en calidad de variable criptográfica. La función criptográfica podría cifrar también algunos o la totalidad de los datos a proteger, usando la clave criptográfica. La función criptográfica puede configurarse así para dar salida a un valor *hash* y/o un texto cifrado de los datos a proteger. Si a algunos de los datos a proteger solamente se les aplica una función *hash* (pero no se cifran), estos datos se deben incluir en la primera parte del paquete de datos como texto en claro en el mismo formato que cuando se usan como entrada para la función criptográfica (*hashing*), con el fin de permitir a la autoridad de autenticación comprobar la congruencia de los datos en texto en claro con el valor *hash*. Sin embargo, si los datos están cifrados, lo cual significa que es posible que la autoridad de autenticación recupere los datos originales a partir del código de autenticación digital mediante descifrado, no es necesario incluirlos en el paquete de datos necesariamente en el mismo formato que cuando se usan como entrada para la función criptográfica (es decir, típicamente en texto en claro).

Merece la pena recordar que el código de autenticación digital puede contener algunos otros datos además de los datos de posicionamiento y del identificador público del receptor. En este caso, la autoridad de autenticación puede confirmar que estos datos adicionales fueron procesados por el receptor en un cierto momento y en una cierta ubicación. Otro aspecto que merece la pena mencionar es que el paquete de datos se puede cifrar (en su totalidad o en parte) por parte del usuario después de que haya sido producido, por ejemplo, con el fin de proteger la privacidad del usuario. Es necesario entonces descifrar el paquete de datos antes de que el mismo se presente para su autenticación a la autoridad de autenticación o a esta última se le debe proporcionar la clave para descifrar el paquete de datos, de manera que la autoridad de autenticación pueda recuperar el contenido del texto en claro y el código de autenticación digital.

La clave criptográfica usada para la función *hash* y/o para cifrar los datos a proteger comprende preferentemente una concatenación de testigos criptográficos difundidos a través de las diferentes fuentes de señales de radionavegación. Sin embargo, la clave criptográfica también puede obtenerse mediante una función más complicada de los testigos criptográficos (por ejemplo, incluyendo permutación o mezclado de los testigos, etcétera). La función que se usa para generar la clave criptográfica a partir de los testigos es conocida solamente para la autoridad de autenticación, la cual, tras solicitársele que autentique un paquete de datos presentado a la misma, recupera los testigos criptográficos correspondientes a la posición geográfica y el tiempo supuestos (a partir de un archivo o usando un algoritmo secreto), con la finalidad de reconstruir la clave criptográfica usada por la función criptográfica del receptor.

El receptor de señales de radionavegación puede haber almacenado una clave secreta, a la que se le denomina posteriormente como identificador secreto del receptor, conocida para la autoridad de autenticación solamente (la clave secreta es un “secreto compartido” del receptor - no del usuario - y la autoridad de autenticación). Puede ser almacenada por ejemplo dentro del receptor por su fabricante bajo un acuerdo de licencia con la autoridad de autenticación. En tal caso, la función usada para generar la clave criptográfica puede usar el identificador secreto del receptor como entrada además de los testigos criptográficos. La clave criptográfica podría ser, por ejemplo, una concatenación de los testigos criptográficos y la totalidad o parte de la clave secreta. Esta opción es especialmente ventajosa para garantizar una longitud constante de las claves criptográficas en caso de pluralidad de testigos criptográficos, dado que el número de fuentes con visibilidad desde el receptor puede variar en el tiempo y en función de la ubicación. De hecho, en caso de un GNSS, por ejemplo, el número de satélites de radionavegación bajo visibilidad del receptor no es constante. Por lo tanto, si la clave criptográfica se obtuviera, por ejemplo, mediante concatenación de solamente los testigos criptográficos, la longitud de la clave variaría y también lo harían la fuerza de la clave criptográfica y la robustez del código de autenticación. Así, la clave criptográfica preferentemente tiene una longitud fija (número de bits), seleccionándose dicha longitud de manera que sea suficiente para un cifrado robusto. El receptor usa de este modo ventajosamente una parte del identificador secreto del receptor para rellenar cualesquiera bits vacíos, es decir, para llegar a la longitud predefinida de la clave criptográfica.

Preferentemente, en caso de una pluralidad de testigos criptográficos, el paquete de datos contiene en su primera o segunda parte datos que identifican aquellas fuentes de señales que difunden los testigos criptográficos usados por

el receptor para calcular la clave criptográfica ("datos de identificación de fuentes de señales"). Esta opción es especialmente preferida, puesto que el tiempo y la ubicación aseverados no son suficientes en todos los casos para que la autoridad de autenticación determine qué testigos criptográficos han sido recuperados realmente por el receptor de radionavegación. La información de tiempo y ubicación de hecho permite establecer qué fuentes de señales eran teóricamente visibles para el receptor. No obstante, la recepción de señales de radionavegación de algunas de estas fuentes podría haberse evitado (por ejemplo, debido al enmascaramiento). En ausencia de indicaciones adicionales sobre qué testigos criptográficos usó realmente el receptor, la autoridad de autenticación tendría que comprobar muchas de las combinaciones teóricamente posibles de testigos criptográficos hasta que halle el que se usó para generar la clave criptográfica. Por contraposición, si las fuentes de los testigos criptográficos se indican en el paquete de datos, la autoridad de autenticación puede identificar rápidamente los testigos criptográficos sobre la base de los datos de posicionamiento (tiempo y ubicación) y los datos que identifican las fuentes de señales. Una vez que los testigos criptográficos han sido identificados, la autoridad de autenticación puede comprobar la congruencia de los datos a proteger y el código de autenticación digital, y emitir un certificado que autentique los datos para protegerlos o declararlos no válidos.

Tal como ya se ha indicado anteriormente, el receptor de señales de radionavegación preferentemente comprende un perímetro de seguridad dentro del cual se llevan a cabo por lo menos las etapas críticas en cuanto a seguridad. Estas etapas incluyen, por ejemplo: recuperar los testigos criptográficos a partir de las señales de radionavegación, determinar los datos de posicionamiento y generar el código de autenticación digital. Una huella digital de software del receptor se puede incluir en el código de autenticación digital. En este caso, dentro del perímetro de seguridad se lleva a cabo también la etapa de calcular la huella digital de software. Los expertos tendrán conocimiento de qué etapas se llevan a cabo preferentemente dentro del perímetro de seguridad para vencer ataques.

En una variante de la invención, los datos de posicionamiento se calculan no solamente a partir de mediciones de pseudodistancias sino también de mediciones de fase.

Como alternativa, el receptor puede calcular datos de posicionamiento a partir de mediciones de pseudodistancias y, posiblemente, mediciones de fase, de señales tanto abiertas como cifradas. El receptor puede configurarse para detectar incongruencias entre los datos de posicionamiento obtenidos a partir de observables de señales abiertas y datos de posicionamiento obtenidos a partir de observables de señales cifradas. Si las posiciones geográficas calculadas difieren en más de un umbral aceptable, el receptor puede decidir descartar las mediciones realizadas sobre señales abiertas y/o incluso activar una alerta que presuponga un ataque de suplantación de identidad sobre las señales abiertas si la incongruencia no puede explicarse por perturbaciones normales tales como multi-trayectos.

Ventajosamente, el receptor también puede calcular datos de posicionamiento basándose en mediciones de multi-frecuencia, es decir, usando señales de radionavegación difundidas en frecuencias diferentes. En algunas circunstancias, es posible que el receptor pueda detectar ataques de retransmisión de señales falseadas, es decir, señales que vuelven a ser difundidas por un emisor con base terrestre con o sin la introducción de un retardo de tiempo. En un ataque de retransmisión de señales falseadas, los mensajes de datos de las señales de radionavegación permanecen invariables. Todas las señales, ya sean abiertas o cifradas, están expuestas a la amenaza de ser retransmitidas como señales falseadas. Un ataque de retransmisión de señales falseadas se puede detectar cuando por lo menos una de las frecuencias de radionavegación disponibles no se retransmite como señal falseada. El receptor puede configurarse así para calcular datos de posicionamiento para las diferentes frecuencias por separado, o para diferentes combinaciones de frecuencias, y para comprobar cualquier incoherencia de los diferentes datos de posicionamiento calculados (sustancialmente) al mismo tiempo.

En este contexto, puede merecer la pena señalar que el uso de señales de radionavegación cifradas no elimina la amenaza de un ataque de interferencias deliberadas. Sin embargo, las interferencias deliberadas pueden detectarse de forma relativamente fácil por medio de un receptor de señales de radionavegación del estado de la técnica.

En el código de autenticación digital se pueden incluir ventajosamente datos relativos a alertas activadas por el receptor como parte de los datos a proteger por el receptor. Los datos pueden ser recopilados por la autoridad de autenticación y se pueden usar para construir una base de datos. La base de datos podría ser monitorizada por la autoridad de autenticación u otro proveedor de servicios para localizar amenazas detectadas. Las interferencias deliberadas, la suplantación de identidad, la retransmisión de señales falseadas u otros ataques detectados podrían así ser comunicados por la autoridad de autenticación a las autoridades nacionales competentes para localizar e, idealmente, neutralizar al atacante.

Volviendo a continuación específicamente al segmento terrestre, un aspecto de la invención se refiere a una autoridad de autenticación tal como ya se ha mencionado en varias ocasiones anteriormente en la presente. La autoridad de autenticación lleva a cabo un procedimiento de comprobación de la autenticidad de los datos a proteger incluidos en un paquete de datos presentado a la misma. Este procedimiento comprende recibir un paquete de datos que ha sido, o que tiene el aspecto de haber sido, producido de acuerdo con el procedimiento según se ha descrito anteriormente en la presente. Se supone que el paquete de datos presentado a la autoridad de autenticación incluye datos de posicionamiento y un código de autenticación digital, en el que los datos de posicionamiento representan la posición geográfica y el tiempo supuestos, y en el que el código de autenticación tiene por lo menos el aspecto de

ser uno de ellos. (Si un paquete de datos presentado a la autoridad de autenticación se encuentra claramente en un formato incorrecto, no existe necesidad de continuar. A continuación el procedimiento de autenticación se puede abortar y se puede emitir un mensaje de error para aquel que haya presentado el paquete de datos). La autoridad de autenticación recupera el testigo o testigos criptográficos que habría recibido un receptor de señales de radionavegación si el mismo hubiera estado realmente en la supuesta posición geográfica y en el tiempo supuesto. La autoridad de autenticación comprueba si los datos de posicionamiento y el código de autenticación digital son congruentes entre sí. Finalmente autentica el paquete de datos (incluyendo la indicación de tiempo-y-ubicación contenida en los datos de posicionamiento) si los datos de posicionamiento y el código de autenticación digital son congruentes entre sí, o rechaza el paquete de datos como no válido si los datos de posicionamiento y el código de autenticación digital no son congruentes entre sí. El certificado, cuando es positivo, puede contener, si fuera necesario, una indicación del nivel de confianza que puede atribuirse a los datos de posicionamiento, basándose, por ejemplo en el número de señales autenticadas usadas para el punto de posición.

Se observará que el procedimiento llevado a cabo por la autoridad de autenticación se ajusta al formato del paquete de datos, que debe ser determinado con antelación por medio de un patrón.

Un proveedor de servicios externo (por ejemplo, una compañía de seguros del tipo “pago-como-conduzco”, o una organización encargada del peaje, etcétera) puede recibir paquetes de datos de sus abonados. El mismo puede presentar los paquetes de datos a la autoridad de autenticación para autenticarlos. La autoridad de autenticación a continuación devuelve un certificado al solicitante que ha presentado un paquete de datos exponiendo si el paquete de datos, en particular la indicación de fecha-y-hora contenida en él, es auténtico. El proveedor de servicios externo podría presentar cada paquete de datos que recibe de sus abonados a la autoridad de autenticación para autenticarlos. Alternativamente, puede presentar muestras seleccionadas aleatoriamente entre todos los paquetes de datos que recibe. El proveedor de servicios externo también puede examinar los paquetes de datos en relación con irregularidades y preferentemente presentar paquetes de datos aparentemente irregulares a la autoridad de autenticación.

La autoridad de autenticación preferentemente determina los valores de los testigos criptográficos que van a ser distribuidos por medio de las fuentes de radionavegación. Después de su generación en la autoridad de autenticación, los testigos criptográficos son transmitidos, a través de una comunicación segura, a estaciones de enlace ascendente, que cargan el testigo en las fuentes de señales de radionavegación, por ejemplo, los satélites. Alternativamente, los testigos criptográficos son generados fuera de la autoridad de autenticación, por ejemplo, por uno o más centros de mando del sistema de radionavegación, y se transmiten usando una comunicación segura a la autoridad de autenticación para su almacenamiento en un archivo y a las estaciones de enlace ascendente para su carga en las fuentes de señales de radionavegación.

En lugar de almacenar todos los testigos criptográficos pasados, la autoridad de autenticación podría recurrir a una función de generación que dé salida a los testigos criptográficos correspondientes a un cierto tiempo. En esta variante, la autoridad de autenticación preferentemente se prepara para cambiar la función de generación, o sus parámetros, de vez en cuando. La autoridad de autenticación debe mantener entonces un archivo de las funciones de generación o los ajustes de los parámetros y sus correspondientes periodos de tiempo.

Debería indicarse que puede haber más de una autoridad de autenticación. En caso de una pluralidad de autoridades de autenticación, existe preferentemente un archivo común de testigos criptográficos o un centro de cálculo común para calcular testigos criptográficos correspondientes a un cierto tiempo, disponiendo de un acceso seguro a dicho archivo o centro de cálculo todos los servicios de autenticación. Alternativamente, cada autoridad de autenticación podría tener su propio archivo o centro de cálculo. Sea cual sea la opción que se selecciones, se debe tener cuidado en mantener los testigos criptográficos y/o su función de generación en secreto. Esto puede resultar más sencillo con una única autoridad de autenticación.

En el segmento de fuentes de señales, un aspecto de la invención son las fuentes de señales de radionavegación, que difunden señales de radionavegación que contienen uno o más testigos criptográficos protegidos mediante cifrado, actualizándose los testigos criptográficos de vez en cuando.

Otro aspecto de la invención se refiere a las propias señales de radionavegación y al uso de dichas señales, por ejemplo, para proporcionar una indicación de tiempo-y-ubicación autenticable. Las señales de radionavegación se caracterizan por uno o más testigos criptográficos incorporados dentro de su contenido de datos y protegidos mediante cifrado.

Los expertos apreciarán que los diferentes aspectos de la presente invención establecen un planteamiento integrado para proporcionar a usuarios de un sistema de radionavegación (usuarios finales así como proveedores de servicios externos) un alto nivel de seguridad.

El uso de señales de radionavegación cifradas, posiblemente sobre múltiples frecuencias y/o en combinación con señales de radionavegación abiertas, de un receptor a prueba de manipulaciones indebidas y el software del receptor concederán una alta confianza en los datos de posicionamiento. En caso de un ataque sobre las señales de

radionavegación (por ejemplo por interferencias deliberadas, suplantación de identidad o retransmisión de señales falseadas), un receptor que funcione de acuerdo con lo dicho anteriormente dispone de la mejor posibilidad de detectar el ataque y alertar al usuario. Además, un usuario puede determinar fácilmente si su receptor funciona correctamente mediante el envió de un paquete de datos a la autoridad de autenticación. Puesto que el receptor podría configurarse para enviar regularmente un paquete de datos a la autoridad de autenticación, por ejemplo, cuando se descargan las claves para acceder a señales de radionavegación cifradas y/o los testigos criptográficos.

La invención permite a cualquiera que esté en posesión de un paquete de datos, obtener confirmación de si el receptor con el cual el paquete de datos afirma haber sido producido, se encontraba en la posición aseverada y en el tiempo aseverado. Si el paquete de datos contiene datos adicionales (por ejemplo, un documento), el solicitante del paquete de datos a la autoridad de autenticación también puede recibir la confirmación de que los datos adicionales fueron empaquetados por el receptor en la ubicación y en el tiempo aseverados.

La invención proporciona así un aumento de la cadena de confianza, dentro de la infraestructura de un sistema de radionavegación (por ejemplo, el futuro GNSS europeo o una red de pseudolites) desde las señales en el espacio al destinatario de un paquete de datos que contiene una indicación de tiempo-y-ubicación. En este sentido, la invención logra la autenticación de datos de posicionamiento de extremo-a-extremo, lo cual representa un paso significativo hacia la radionavegación segura.

La invención aumenta la robustez de la radionavegación ante amenazas malintencionadas sobre señales de radionavegación y garantiza la protección de datos de posicionamiento ante intentos malintencionados de alterarlos y proporciona unos medios para el geoetiquetado y el etiquetado en el tiempo de cualquier tipo de documentos de una manera segura.

La invención puede combinarse beneficiosamente con una aplicación que aumente la precisión de posicionamiento a través de la entrega segura de datos de corrección, permitiendo unos medios seguros y más precisos de posicionamiento y temporización.

Breve descripción de los dibujos

A continuación se describirá una forma de realización preferida de la invención, a título de ejemplo, en referencia a los dibujos adjuntos en los cuales:

La figura 1 es una ilustración esquemática de un GNSS configurado según la presente invención;

la figura 2 es un diagrama de bloques esquemático del software del receptor;

la figura 3 es una ilustración de un paquete de datos autenticable;

la figura 4 es una ilustración del cálculo de una clave de cifrado sobre la base de los testigos criptográficos recuperados por un receptor GNSS.

Descripción de formas de realización preferidas

Introducción

En lo sucesivo, se abordará más detalladamente una posible implementación de la invención, usando el Servicio Comercial (CS) del GNSS europeo (conocido como Galileo). El ejemplo del Servicio Comercial se ha elegido en este caso principalmente porque constituirá el primer servicio GNSS que ofrezca a usuarios civiles señales de radionavegación cifradas, la cual probablemente es la manera más práctica y segura de lograr la autenticación de SIS autónoma.

El ejemplo que se describe en la presente en lo sucesivo explica los diferentes aspectos de la invención con más detalle. El ejemplo se refiere a la producción, por parte de un receptor de señales de radionavegación, de resúmenes digitales con la entrada de testigo(s) criptográfico(s) incorporado(s) en el mensaje de datos de señales de navegación de CS con la finalidad de autenticar:

- los datos de posicionamiento producidos por un receptor de radionavegación autorizado, sobre la base de señales de radionavegación difundidas por un sistema de navegación local, regional o global por satélite o un sistema de pseudolites con base terrestre;
- y la identidad del receptor de radionavegación y, cuando resulte apropiado, la identidad del usuario del receptor y/o cualquier tipo de autorización administrativa otorgada al mismo;
- y/o, cuando resulte apropiado, documentos de cualquier clase, que sean geoetiquetados y etiquetados en el tiempo por el receptor.

Arquitectura del sistema

La arquitectura del ejemplo se ilustra en la figura 1. El GNSS comprende un segmento terrestre 10, que se encarga de, entre otros aspectos, la sincronización de todos los satélites 12 y/o pseudolites (no mostrados) y la preparación del mensaje de datos que se va a difundir sobre las señales de radionavegación. El segmento terrestre 10 incluye varias estaciones de enlace ascendente 14 controladas por una autoridad de autenticación de confianza, denominada, en lo sucesivo en la presente, Centro de Servicio de Autenticación 16.

El GNSS también comprende un segmento espacial 18 con una pluralidad de satélites de radionavegación 12 orbitando en una órbita terrestre media sobre tres o seis planos orbitales diferentes y/o una pluralidad (más de 5) de pseudolites sincronizados.

El segmento de usuario 20 del GNSS comprende receptores de radionavegación de usuarios 22.

Los usuarios pueden ser abonados de un proveedor de servicios externo 24, que proporcione servicios geo-localizados.

Existe un segmento de telecomunicaciones 26 para la transmisión de paquetes de datos desde receptores de abonados 22 a los proveedores externos 24 (la “red por paquetes de datos”) y un segmento de telecomunicaciones seguras 28 para la distribución de las claves de navegación (“navkeys”) desde el Centro de Servicio de Autenticación 16 a los receptores de usuario (la “red de *navkeys*”).

El Centro de Servicio de Autenticación 16 garantiza:

- la provisión de testigos criptográficos;
- la provisión de números de identificación secretos para los receptores 22;
- la autenticación de los paquetes de datos producidos por los receptores 22;

El segmento terrestre 10 asigna algo de espacio dentro de los mensajes de datos de las señales de radionavegación de CS para la difusión de testigos criptográficos. El mismo cifra los mensajes de datos completos antes de cargarlos en los satélites 12 o garantiza que los satélites 12 cifren las señales de radionavegación.

El Centro de Servicio de Autenticación 16 produce testigos criptográficos a través de un algoritmo del estado de la técnica. La frecuencia de actualización de las claves criptográficas que se obtienen a partir de los testigos depende del nivel de robustez buscado. Esta frecuencia se verá limitada por el nivel de disponibilidad de estaciones de enlace ascendente 14 y de su conectividad con los satélites 12: de hecho los mensajes de datos se cargan - y por lo tanto se actualizan - a través de estaciones de enlace ascendente, en los satélites en instantes de tiempo diferentes.

El Centro de Servicio de Autenticación 16 mantiene un archivo de todos los testigos criptográficos que ha producido.

El Centro de Servicio de Autenticación 16 tiene un enlace de comunicaciones seguro 30 con el segmento de misión terrestre del sistema Galileo, que controla las estaciones de enlace ascendente, para la transmisión de los testigos, desde el Centro de Servicio de Autenticación al segmento terrestre; y para la transmisión de los testigos leídos por estaciones sensoras o de monitorización desde el segmento de misión terrestre al Centro de Servicio de Autenticación.

Los receptores de usuario 22 están equipados con un hardware específico (módulo criptográfico) y un software específico para recuperar los testigos criptográficos a partir de las señales de radionavegación de CS, para generar un código de autenticación digital usando una función criptográfica que toma como entradas por lo menos los datos de posicionamiento calculados por el receptor y los testigos criptográficos, y para proporcionar un conjunto de datos que incluye por los datos de posicionamiento y el código de autenticación digital.

Proveedores de servicios externos 24 pueden solicitar la autenticación de paquetes de datos de sus abonados al Centro de Servicio de Autenticación 16. El Centro de Servicio de Autenticación 16 a continuación comprueba si los datos de posicionamiento (y posiblemente otros datos a proteger) son congruentes con el código de autenticación digital contenido en el paquete de datos y devuelve al proveedor de servicios externo un certificado que indica el resultado de la verificación.

Distribución de los testigos criptográficos

El mensaje de datos de cada una de las señales de radionavegación producidas por el segmento espacial asigna un número fijo de bits para el testigo criptográfico. Esta longitud se determina por el nivel de robustez previsto para la aplicación. Esta longitud no se debería cambiar; si no, el software de todos los receptores dedicados debe actualizarse para tener en cuenta este cambio en la estructura del mensaje de datos.

Los valores de los testigos criptográficos se cambian en ciertos intervalos de tiempo con el fin de vencer a un pirata informático que desee piratear el cifrado usado para la producción de un código de autenticación digital. La frecuencia de actualización quedará limitada por la capacidad física de los segmentos terrestre y espacial.

El mensaje de datos contiene todos los datos necesarios para permitir que el receptor materialice un punto de posición con las señales de radionavegación cifradas que transportan los testigos criptográficos.

El Servicio Comercial del GNSS europeo usa señales de radionavegación cifradas en la banda de frecuencias E6B. El mensaje de datos de las señales E6B puede usarse para difundir los testigos criptográficos. Así, en la siguiente descripción, se supone que se difunden testigos criptográficos en el mensaje de datos E6B.

Según el Documento de Requisitos de la Misión v7.0, el cifrado del código de determinación de la distancia del GNSS europeo en las señales E6B (canal de datos) y E6C (señal piloto sin canal de datos) se basa en un algoritmo simétrico robusto de la Norma de Cifrado Avanzado (AES) con claves de 256 bits. El algoritmo se usa en modo de Contador. Las claves secretas necesarias para que los receptores GNSS accedan a las señales de radionavegación cifradas, es decir, las claves de navegación, son gestionadas y distribuidas por el Centro de Servicio de Autenticación a los usuarios y se renuevan entre cada semana y cada 3 meses. A efectos de su distribución, las claves de navegación se cifran con el ID Secreto del Receptor y se envían al receptor a través de Internet. Si el receptor no tiene ninguna interfaz directa con Internet, las claves de navegación son enviadas en una primera etapa a un ordenador personal y en una segunda etapa se cargan en el receptor, por ejemplo, con una unidad de almacenamiento flash USB. En la presente se supone que la longitud del ID Secreto del Receptor equivale a 256 bits.

Tal como se ha indicado anteriormente en la presente, una señal de radionavegación se califica como segura si se cumple una de las siguientes condiciones:

(a) la señal de radionavegación está cifrada en sí misma (es decir, el código de determinación de la distancia de la señal está cifrado) con un algoritmo de cifrado del estado de la técnica, o

(b) la señal de radionavegación no está cifrada pero el mensaje de datos (incluyendo los testigos criptográficos) que transporta está cifrado con un algoritmo de cifrado del estado de la técnica; o

(c) tanto la señal de radionavegación como su mensaje de datos están cifrados con el mismo algoritmo de cifrado del estado de la técnica o dos algoritmos de cifrado diferentes, con dos series de claves diferentes.

Así, las señales E6 permiten realizar mediciones de pseudo-distancias totalmente fiables (a diferencia de las señales E1, a las que se puede aplicar fácilmente una suplantación de la identidad) y por lo tanto calcular una PVT igualmente totalmente fiable.

El Centro de Servicio de Autenticación del Servicio Comercial del Galileo calcula un testigo criptográfico para cada satélite y para cada período de validez de los testigos criptográficos. Estos testigos criptográficos se cargan en los satélites a través de una estación de enlace ascendente y a continuación son difundidos por los satélites.

Cada satélite SVi (siendo i el número del satélite o “vehículo espacial”) difunde un testigo criptográfico específico, denominado, en la presente en lo sucesivo, “$NONCE_{SVi}$”, en el mensaje de datos. La longitud de cada $NONCE_{SVi}$ podría ser por ejemplo de 32 bits.

El mensaje de datos comprende, entre otros, dentro de 448 bits:

- el mensaje de navegación para E6B. Esto permitirá a los receptores continuar con la navegación incluso en un entorno en el que las señales E1A y E5A sean atacadas o bien por interferencias deliberadas o bien por suplantación de identidad. Esto ocupará como mucho 50 bits por segundo del ancho de banda de datos de 448 bits por segundo en E6B.

- Datos adicionales que permiten que el receptor reconstruya el mensaje de navegación para E1A, permitiendo la navegación en E6B y E1A, incluso en casos en los que E1A sufra un ataque de suplantación de identidad. Un valor impredecible para cada nuevo testigo criptográfico ($NONCE_{SVi}$).

$NONCE_{SVi}$ es específico del satélite SVi. Por lo tanto, normalmente: $NONCE_{SVi}(t) \neq NONCE_{SVj}(t)$, si $i \neq j$. Sin embargo, puede haber ocasiones en las que dos o más testigos criptográficos sean accidentalmente iguales.

El Centro de Servicio de Autenticación archiva todos los *nonces* criptográficos en un archivo (“el archivo NONCEs”).

Cálculo de paquetes de datos por parte del receptor

La figura 2 ofrece una visión general de una posible implementación del software del receptor. El software

comprende cuatro componentes principales:

- el software de autenticación de SiS;
- el software de gestión de claves;
- el software de cifrado/descifrado;
- el software de navegación.

Las claves necesarias para que los receptores de usuario accedan a la señal de radionavegación y/o los testigos criptográficos se transmiten a través de una red de comunicaciones segura y se gestionan dentro del receptor en un módulo criptográfico y el software de gestión de claves.

El software del receptor se basa ante todo en las mediciones de pseudo-distancias calculadas sobre la base de las señales de radionavegación seguras. Solamente los datos de posicionamiento obtenidos a partir de señales de radionavegación seguras se pueden considerar como seguros.

Además de las entradas habituales proporcionadas por el mensaje de navegación de cada señal de radionavegación, se pueden añadir datos adicionales en el mensaje de datos de las señales de radionavegación seguras con el fin de colaborar con el software de navegación. Por ejemplo, el software de navegación del receptor puede tener en cuenta:

- datos de integridad entregados por el operador GNSS a través de las señales de radionavegación seguras;
- datos de corrección de la navegación proporcionados por el operador GNSS o por el Centro de Servicio de Autenticación;
- diferenciales de reloj con otra(s) frecuencia(s) del segmento espacial.

El software de navegación podría configurarse para la Monitorización Autónoma de la Integridad en el Receptor (RAIM) y/o comprender una función de aumentación (alimentada por datos de corrección) tal como, por ejemplo, el Posicionamiento Puntual Preciso.

El receptor produce un paquete de datos que comprende dos partes:

- La parte 1 comprende “información legible”, que contiene datos en “texto en claro”, incluyendo datos de posicionamiento.
- La parte 2 es el denominado “código de autenticación digital”.

El código de autenticación digital permite al Centro de Servicio de Autenticación autenticar los datos a proteger. El código de autenticación digital puede comprender parte o la totalidad de los datos a proteger. Si el código de autenticación digital contiene un valor *hash* de ciertos datos, estos datos tienen que estar presentes en la parte de texto en claro (parte 1). Si no, el Centro de Servicio de Autenticación no podrá comprobar el código de autenticación digital.

Es posible incluir datos tanto en la parte 1 como en la parte 2 del paquete de datos. Aunque es cierto que esto en general duplica la información, puede resultar interesante que algunas aplicaciones puedan recuperar los datos contenidos en el código de autenticación digital, en situaciones en las que este último no concuerde con la parte 1.

Volviendo a continuación al receptor preferido de radionavegación ilustrado en la figura 3, el mismo es un receptor GNSS por lo menos bi-frecuencia, a prueba de manipulaciones indebidas (bandas E1A/E6B). Preferentemente, el receptor está configurado para gestionar señales de radionavegación E1, E5 y E6. El perímetro de seguridad del receptor incluye por lo menos los correladores E6 y procesado de banda base.

El receptor también está equipado con un sistema de navegación inercial (INS). Además, el receptor está equipado con una ranura USB. El usuario inserta una unidad de almacenamiento flash USB dedicada en la ranura para cargar las claves de navegación. La unidad de almacenamiento flash USB también puede usarse para transferir otros datos al receptor, tales como por ejemplo el ID Público de Usuario, que podría ser por ejemplo un permiso de conducción.

La unidad de almacenamiento flash USB también almacena todos los paquetes de datos, o por lo menos una muestra de ellos en un intervalo predeterminado, durante un periodo predeterminado. Todos los paquetes de datos se almacenan en formato cifrado para proteger la privacidad, en caso de que por ejemplo la unidad de almacenamiento flash USB sea robada. Los paquetes de datos pueden transferirse desde la unidad de almacenamiento flash USB al Centro de Servicio de Autenticación a través del ordenador personal del usuario, cada vez que el usuario solicite en el sitio web del Centro de Servicio de Autenticación las siguientes claves de navegación. La transferencia de paquetes de datos posibilita que el Centro de Servicio de Autenticación lleve a cabo una autenticación remota de PVT *a posteriori*. Para esta aplicación (es decir, autenticación remota de PVT en

diferido) el Centro de Servicio de Autenticación envía - con la autorización del usuario - todos los paquetes de datos y sus correspondientes certificados a los proveedores de servicios del usuario.

El receptor puede estar equipado con un terminal para telecomunicaciones inalámbricas tales como GPRS, G3 o G4. Este enlace de telecomunicaciones se usa para lograr la autenticación de PVT en tiempo casi real para un tercero. Esta función (es decir, la autenticación remota de PVT en tiempo casi real) sería muy valiosa para el seguimiento en tiempo real de bienes preciados o de personas en libertad condicional, aunque resultaría menos interesante para aplicaciones tales como la tarificación de conductores o planes de seguros del tipo pago-como-conduzco.

El ID Público de Receptor preferentemente se marca en el receptor de forma visible.

El ID Privado de Receptor se almacena en una memoria a prueba de manipulaciones indebidas. No es conocido ni por el usuario ni por ningún otro participante, exceptuando el Centro de Servicio de Autenticación.

El software del receptor se almacena en la misma u otra memoria a prueba de manipulaciones indebidas. Preferentemente, las memorias para el software del receptor y el ID Privado de Receptor, respectivamente, son independientes, con el fin de evitar el borrado potencial del ID Privado de Receptor durante una actualización del software.

El receptor preferentemente se alimenta mediante un cable de alimentación seguro de manera que no se pueda desconectar físicamente.

El receptor también podría estar equipado con un emisor de DSCR que transmite a corta distancia la información sobre si el receptor está encendido y funcionando correctamente. Estas medidas pueden evitar que un usuario desactive voluntariamente su receptor para evitar pagos o penalizaciones debido a un proveedor de servicios.

El software del receptor tiene cuatro bloques funcionales principales:

- el software de navegación encargado del cálculo de PVTs de las señales de navegación;
- el software de gestión de claves encargado de cargar las claves de navegación cifrada desde la unidad de almacenamiento flash USB del usuario;
- el software de autenticación de SIS encargado de detectar ataques por interferencias deliberadas, por suplantación de identidad y por retransmisión de señales falseadas;
- el software de descifrado/cifrado encargado de producir el “código digital de autenticación” y de descifrar claves de navegación cifradas.

El receptor asigna dos canales de correlación a cada satélite (uno en E1A y otro en E6B). El receptor adquiere a continuación los códigos de determinación de la distancia en E1A y E6B, lee el mensaje de navegación en E1 y E6B, y extrae del mensaje de datos de E6B el *nonce* difundido por el satélite.

El software de navegación calcula dos soluciones de PVT, la primera de ellas sobre la base de señales de E6B solamente y la segunda se basa en todas las señales disponibles, incluyendo E1 y E6.

A la primera PVT se le denomina PVTE6. Se calcula usando solamente mediciones de pseudo-distancias de E6B (PRE6).

A la segunda PVT se le denomina PVTE1, E6. Se basa en mediciones de pseudo-distancias sin efecto ionosférico (a las que se hace referencia como PRionofree), las cuales se calculan según la fórmula:

$$PR_{ionofree} = \frac{f_{E1}^2}{f_{E1}^2 - f_{E6}^2} PR_{E1} - \frac{f_{E6}^2}{f_{E1}^2 - f_{E6}^2} PR_{E6},$$

en la que f_{E1} es la portadora de frecuencia E1A del Galileo (1.575,42 MHz), f_{E6} es la portadora de frecuencia E6B del Galileo (1.278,750 MHz), PR_{E1} es la pseudo-distancia de E1 y PR_{E6} es la pseudo-distancia de E6.

El software de navegación puede estimar una “caja de confianza” tetradimensional centrada en PVT_{E6}, y definida por las dimensiones de tiempo, horizontal y vertical. Tiene en cuenta todos los errores posibles en una navegación basada en E6B solamente. Las cuatro dimensiones de la caja de PVT de confianza pueden calcularse por medio del receptor sobre la base de datos proporcionados por el Centro de Servicio de Autenticación sobre el estado de la constelación.

El tamaño de la caja de PVT de confianza puede reducirse significativamente si el software se combina con un servicio de alta precisión en E6B permitiendo que el receptor se beneficie de una mayor precisión de las posiciones de los satélites (efemérides de alta precisión) y de derivas de los relojes de los satélites.

Puede que merezca la pena señalar que $PVT_{E1, E6}$ es más precisa pero no totalmente segura en comparación con PVT_{E6} mientras que PVT_{E6} es menos precisa pero totalmente fiable. La posición PVT_{E6} es la única solución fiable puesto que se calcula sobre la base de las señales seguras y de confianza (ya que estas últimas están cifradas). Esta posición-tiempo es precisa dentro de márgenes de error determinados en la totalidad de las cuatro dimensiones Dx, Dy, Dz y Dt.

La caja de confianza indica que la posición y el tiempo verdaderos del receptor (PVT_{exacta}) están contenidos en la caja de confianza con una probabilidad predefinida (nivel de confianza).

Las dimensiones de la caja de confianza dependen de la configuración de la constelación del Galileo en el instante de tiempo en cuestión. Las dimensiones de la caja podrían reducirse significativamente si el sistema se combina con una aplicación de alta precisión aplicada en E6B.

Si se suplanta la identidad de señales E1, el receptor o bien no podrá calcular $PVT_{E6, E1}$ y por lo tanto activará una alerta de suplantación de identidad, o bien podrá calcular $PVT_{E6, E1}$, que es probable que se sitúe fuera de la caja de PVT de confianza. Si $PVT_{E6, E1}$ se sitúa de hecho fuera de los límites de la caja de PVT de confianza, el receptor también activará una alerta.

En caso de una alerta de este tipo, el receptor solamente da salida a PVT_{E6} y a la dimensión de la caja de confianza. Esta última, a continuación, se considerará como la mejor aproximación de la posición y el tiempo verdaderos.

Si no se activa ninguna alerta, el receptor da salida tanto a PVT_{E6} como a $PVT_{E6, E1}$. $PVT_{E6, E1}$ se considerará entonces como la mejor aproximación de la posición y el tiempo verdaderos.

Gestión de las claves de navegación

El usuario puede descargar las claves de navegación de señales E6B a través de Internet de forma regular, una vez al mes por poner un ejemplo. Estas claves serán producidas por el operador del Galileo o alternativamente por el Centro de Servicio de Autenticación.

El operador del Galileo asigna a las cargas útiles de E6B de todos los satélites la misma clave de navegación con el fin de cifrar las señales de navegación con esta clave de navegación única. La solución de autenticación descrita en este caso también podría funcionar con una clave de navegación diferente asignada a cada satélite.

El usuario descarga las claves de navegación con antelación al cambio. El usuario iniciará sesión en el sitio web seguro de Internet del Centro de Servicio de Autenticación. A tal efecto, se identificará por su nombre de usuario (por ejemplo el ID Público de Receptor) y una contraseña secreta. Cuando se identifique, puede presentar una solicitud para la renovación de la clave e insertar la unidad de almacenamiento flash USB en el ordenador con esa finalidad.

La solicitud es gestionada por el software de base de datos del Centro de Servicio de Autenticación. La base de datos contiene todos los nombres de usuario, contraseñas secretas, IDs Públicos de Receptor e IDs Privados de Receptor. El servidor de base de datos identifica el ID Público de Receptor y así recupera el ID Privado de Receptor correspondiente. El ID Privado de Receptor se usa a continuación para cifrar la clave de navegación con un algoritmo de cifrado simétrico. El sitio web descarga entonces la clave de navegación cifrada en la unidad de almacenamiento flash USB hasta el ordenador personal del usuario.

Mientras tanto, la aplicación del sitio web cargará todos los paquetes de datos almacenados en la unidad de almacenamiento flash USB insertada en el ordenador personal. Posteriormente, estos paquetes de datos son certificados por el Centro de Servicio de Autenticación y a continuación son enviados a los proveedores de servicios externos designados por el usuario.

Cuando las nuevas claves de navegación han sido descargadas en la unidad de almacenamiento flash USB, el usuario inserta la unidad de almacenamiento flash USB en el receptor de señales de radionavegación. Esta inserción activa las siguientes acciones. El software de gestión de claves del receptor comprueba si una clave de navegación cifrada nueva está almacenada en la unidad de almacenamiento flash USB. Si es así, el software carga la clave de navegación cifrada en una memoria dentro del perímetro de seguridad del receptor.

A continuación, el software de descifrado y cifrado descifra la clave de navegación cifrada con la ayuda del ID Privado de Receptor almacenado dentro del perímetro de seguridad y guarda la versión descifrada de la clave de navegación en otra memoria a prueba de manipulaciones indebidas dentro del perímetro de seguridad, junto con los parámetros de validez con el transcurso del tiempo.

El software de gestión de claves elimina las claves de navegación cuya validez haya expirado.

Si es necesario, el software de gestión de claves alerta al usuario, a través de la interfaz del receptor, de la inminente finalización de la validez de la clave de navegación actual y, si fuera necesario, de la ausencia de una clave de navegación válida para el siguiente período de navegación. En ausencia de una clave para el periodo actual, el receptor ya no podrá realizar un seguimiento de señales E6B y adquirirlas. En tal caso, la función de autenticación de SIS autónoma se pierde y la posterior autenticación remota de PVT por parte del Centro de Servicio de Autenticación ya no resulta posible.

Procesado en tiempo real de la autenticación de SIS por parte del receptor

En primera instancia, el software de autenticación de SIS indica al usuario, a través de la interfaz del receptor, desde qué satélites Galileo se han adquirido y descifrado mensajes de datos de E6B, es decir, qué satélites Galileo son visibles desde el receptor cuando éste último calcula la PVT.

La segunda tarea del software de autenticación de SIS es monitorizar y detectar continuamente ataques por interferencias deliberadas. Por ejemplo el software de autenticación de SIS activa una alerta de interferencias deliberadas si el receptor pierde una frecuencia pero sigue recibiendo señales sobre otra frecuencia desde los mismos satélites. Esta alerta indica qué frecuencia se ha perdido.

Si se han perdido señales en la banda de E6B, pero el receptor sigue leyendo señales de E1 o E5, el software de autenticación de SIS activa una alerta indicando que la navegación por satélite ya no es segura y solicita al software de navegación que conmute al modo de navegación INS.

Si las señales de radionavegación se han perdido en todas las frecuencias, el software de autenticación de SIS activa una alerta indicando que ya no es posible la navegación por satélite y también solicita al software de navegación que conmute a la navegación INS.

El software de autenticación de SIS detecta ataques de suplantación de identidad, es decir situaciones en las que un atacante modifica los datos de navegación difundidos sobre señales abiertas. Se activará una alerta de suplantación de identidad por ejemplo cuando las efemérides leídas sobre la señal E1 (no inmune a la suplantación de identidad) sean diferentes de las efemérides leídas sobre E6 (inmune a la suplantación de identidad según el estado actual de la técnica).

El software de autenticación de SIS también puede detectar ataques por retransmisión de señales falseadas en algunas situaciones. Se considera que tiene lugar un ataque por retransmisión de señales falseadas cuando un emisor con base terrestre redifunda señales-en-el-espacio con o sin la introducción de un retardo de tiempo. En un ataque por retransmisión de señales falseadas, los mensajes de datos de las señales-en-el-espacio permanecen invariables. Todas las señales, ya sean abiertas o cifradas como la E6B pueden experimentar un ataque por retransmisión de señales falseadas. Puede detectarse un ataque por retransmisión de señales falseadas cuando por lo menos una de las frecuencias de radionavegación disponibles no ha sufrido este tipo de ataque, por ejemplo cuando PVT_{E1} o PVT_{E5} sale de la caja de PVT de confianza centrada en PVT_{E6}. El software detecta en este caso una incoherencia de posiciones calculadas, cada una de ellas, sobre la base de las señales en una frecuencia a la vez.

Sin embargo, el software de autenticación de SIS no puede detectar un ataque por retransmisión de señales falseadas que modifique en paralelo el retardo de transmisión de señales sobre todas las frecuencias de radionavegación. Dicho esto, la introducción en el receptor de un sistema de navegación inercial (INS) debería permitir en teoría que el receptor detectase dichos ataques. Cuando es sometido a este tipo de ataques, el receptor equipado con algún INS debería detectar una incongruencia entre una nueva PVT calculada sobre la base del INS y de la última PVT, y la PVT calculada sobre la base de las señales de navegación.

El software de autenticación de SIS comprobaría, bajo solicitud, el software embarcado en el receptor con la ayuda de la huella digital almacenada en la unidad de almacenamiento flash USB. Si la SHA256 del software no coincide con la huella digital en cuestión, esto significa que el software instalado a bordo del receptor ha sido modificado y se activará una alerta en relación con la integridad del software.

Encapsulamiento de la PVT por parte del receptor

Además de una posición mostrada sobre un mapa en la pantalla, el receptor produce dentro de su perímetro de seguridad una salida (el paquete de datos) destinada a ser enviada a, y usada por, terceros. El paquete de datos comprende dos partes (véase la figura 3):

- Parte 1 (“la información legible”), que incluye la siguiente información:

- $PVT_{E1, E6}$;
- ID Público de Receptor;
- ID Público de Usuario (opcional);

◦ Parte 2 (“el código de autenticación digital”) es un cifrado de la información siguiente:

- Un campo de 27 bits que identifica satélites Galileo usados para el cálculo de la PVT PVT_{E6};
- PVT_{E6};
- Las dimensiones de la caja de PVT de confianza;
- $PVT_{E1,E6}$;
- ID Público de Usuario (opcional);
- la huella digital del software del receptor calculada con SHA256.

El paquete de datos no se debería partir, truncar o modificar en ningún caso. En caso contrario perdería su carácter autenticable. Por lo tanto, debería producirse, transmitirse, almacenarse y archivarse siempre bajo el mismo formato.

El software de encapsulamiento puede producir la Parte 1 (“la información legible”) o bien en claro o bien cifrada, en función de si el usuario desea proteger su privacidad. El cifrado de la Parte 1 se realiza entonces solamente con el propósito de proteger la privacidad, pero en absoluto con el propósito de autenticar posteriormente el paquete de datos. La posibilidad de cifrar la Parte 1 es un complemento con respecto a la aplicación de autenticación, pero no una de sus características esenciales.

La Parte 1 (“la información legible”) puede ser cifrada o no cifrada, en función de la elección realizada por el usuario en el receptor para proteger su privacidad, ya que la Parte 1 puede ser intervenida por terceros maliciosos en cualquier momento después de que esta información haya abandonado el receptor. Si la Parte 1 está cifrada, se aplicará el siguiente esquema con el fin de gestionar el clan de usuario:

◦ El usuario introduce una clave secreta en el receptor.

◦ A continuación la Parte 1 se cifra con esta clave secreta usando un algoritmo de cifrado simétrico.

◦ El usuario tiene la responsabilidad de distribuir su clave secreta a su tribu y a sus proveedores de servicios de una forma segura.

La Parte 2 (“el código de autenticación digital”) necesariamente está cifrada y no se puede leer, excepto por el Centro de Servicio de Autenticación. El algoritmo de cifrado es, por lo menos, un esquema de cifrado integrado de curva elíptica (ECIES) de 192 bits. Al software que produce la Parte 2 se le denomina en lo sucesivo software de descifrado/cifrado.

El ID secreto del receptor es exclusivo, desconocido para el usuario y para cualquier tercero, y está protegido dentro del perímetro de seguridad del receptor.

La Parte 1 (“la información legible”) está destinada a ser usada por cualquier tercero, incluyendo proveedores de servicios geo-localizados o de temporización, mientras que la Parte 2 que acompañará a la Parte 1 en cualquier circunstancia, puede ser leída y por lo tanto usada solamente por el Centro de Servicio de Autenticación.

Por otra parte, los usuarios pueden transmitir los mismos paquetes de datos (Parte 1 + Parte 2) a un número ilimitado de proveedores de servicios geo-localizados o de temporización y a sus clanes (familiares, amigos, compañeros). Cada uno de los destinatarios de esta información puede de hecho presentar en cualquier momento una solicitud de una autenticación ante el Centro de Servicio de Autenticación, siempre que la Parte 2 haya permanecido unida a la Parte 1.

La tarea principal del software de encapsulamiento es cifrar la información indispensable para la futura autenticación de la PVT encapsulándola en la Parte 2 del paquete de datos en un procedimiento de dos etapas, tal como se describe más adelante.

Todas las operaciones de cifrado se realizan dentro del perímetro de seguridad del receptor.

La Parte 2 (“el código de autenticación digital”) se produce por dos encapsulamientos sucesivos.

El primer encapsulamiento abarca un conjunto de datos compuestos por:

◦ PVT_{E6},
◦ Las cuatro dimensiones de la caja de PVT de confianza,
◦ $PVT_{E1, E6}$,
◦ ID Público de Receptor,

- ID Público de Usuario (opcional),
- la huella digital del software del receptor calculada con SHA256.

Este paquete de datos se cifra a través de un algoritmo de cifrado simétrico con una clave correspondiente a la concatenación en un orden predeterminado de todos los *NONCEs* leídos por el receptor en los mensajes de datos E6B. Este cifrado produce el primer encapsulamiento al que se denomina en lo sucesivo En1.

El cifrado se obtiene por la concatenación de 8 testigos criptográficos de satélites bajo visibilidad en un orden predeterminado, por ejemplo la clasificación creciente de los identificadores de satélites. Si hay menos de 8 satélites Galileo bajo visibilidad para el receptor, el campo de *nonces* que se ha dejado vacío se sustituirá por un extracto del ID Privado de Receptor. Se toma esta precaución con el fin de garantizar para todos los encapsulamientos la máxima robustez con una clave de la longitud máxima (256 bits). La figura 5 ilustra el cálculo de una clave criptográfica (con una longitud de 256 bits) cuando bajo la visibilidad del receptor se encuentran solamente cinco satélites. La clave criptográfica se obtiene mediante concatenación de los testigos criptográficos disponibles ($NONCE_{SVi1}$, ..., $NONCE_{SVi5}$) y una parte del ID Privado de Receptor. El ID Privado de Receptor se trunca de tal manera que se logra una clave con la longitud predefinida.

El segundo encapsulamiento abarca un paquete de datos compuesto por:

- En1;
- un elemento de 27 bits que da a conocer los satélites Galileo usados para calcular la PVT y por lo tanto para cifrar En1 (a través de la concatenación de los NONCEs correspondientes);

En una segunda fase, este paquete se cifra a través de un algoritmo de cifrado simétrico con el ID Secreto de Receptor como clave. Este cifrado produce el segundo encapsulamiento denominado en lo sucesivo En2. En2 es la Parte 2 del paquete de datos (“el código de autenticación digital”).

La Parte 1 (“la información legible”) y la Parte 2 (“el código de autenticación digital”) se ensamblan entonces finalmente en un formato predeterminado en el paquete de datos. El paquete de datos se envía, a continuación, a través de cualquier red de telecomunicaciones, a la que se denomina en lo sucesivo red por paquetes de datos - a todos los proveedores de servicios con los que el usuario ha firmado un contrato o un acuerdo.

Distribución de los paquetes de datos

Los paquetes de datos pueden ser transportados por cualquier tipo de medios. La red por paquetes de datos podría ser típicamente una red terrestre de radiofrecuencia usada para transmisión de datos, tal como GPRS, G3 o G4, que resulten ser convenientes para llegar a vehículos móviles. Se podrían transmitir en tiempo real o en tiempo casi real a un proveedor de servicios externo. Los paquetes de datos también se podrían transmitir en tiempo diferido, preferentemente a intervalos regulares. Esto podría realizarse con una unidad de almacenamiento flash USB e Internet, o por medio de cualquier otra conexión de telecomunicaciones. El proveedor puede solicitar, del Centro de Servicio de Autenticación, la autenticación de los paquetes de datos que recibe (en tiempo real o en tiempo diferido).

La red de *navkeys* y la red por paquetes de datos pueden ser la misma red. Esta situación será más fácil de gestionar dentro del receptor, ya que reduce el número de terminales de telecomunicaciones.

Esta situación también puede presentar otra ventaja para aplicaciones que no requieren una autenticación remota de PVT en tiempo real o en tiempo casi real. En lugar de transmitir paquetes a un número de terceros (proveedores de servicios) interesados en los datos producidos por el receptor, éste último puede enviar todos sus paquetes a un punto focal, el Centro de Servicio de Autenticación, que puede enviarlos a los terceros designados, junto con un certificado. El envío de uno o más paquetes de datos a la autoridad de autenticación puede realizarse condicionado a la entrega de las siguientes claves de navegación. Así, se obligará al usuario a proporcionar, a ciertos intervalos, sus datos de posicionamiento, ya que de lo contrario perderían el acceso a las señales de radionavegación seguras y/o los testigos criptográficos. Otra ventaja de este planteamiento es que el centro de servicio de autenticación puede comprobar la integridad del software de receptor (usando la huella digital de software contenida en el código de autenticación digital) y que así se puede evitar distribuir las claves de navegación a receptores con un perímetro de seguridad pirateado.

Protección de la PVT después de su cálculo

El receptor produce el paquete de datos, formado por dos partes:

- La Parte 1 es la “información legible”, que contiene la PVT en texto en claro, proporcionada en un formato predeterminado, y el identificador público del receptor (“el ID Público de Receptor”).
- La Parte 2, el código de autenticación digital que abarca, entre otros, en un formato cifrado, la identificación

del receptor, PVT_{E6} y $PVT_{E6, E1}$ y las dimensiones de la caja de PVT de confianza.

Un segmento de telecomunicaciones con base en tierra (denominado en lo sucesivo red por paquetes de datos) garantiza que la información producida según se ha descrito anteriormente se transmita a cualquier proveedor de servicios basado en la ubicación. La información se puede transportar por cualquier tipo de medios:

- en tiempo (casi) real a través de una red inalámbrica con base terrestre tal como GPRS, G3 o G4;
- o en tiempo diferido, preferentemente a intervalos regulares, a través de las unidades de almacenamiento flash USB e Internet.

Los destinatarios de los paquetes de datos pueden ser proveedores de servicios externos que pueden presentar una solicitud de autenticación al Centro de Servicio de Autenticación. Alternativamente, los paquetes de datos pueden enviarse al Centro de Servicio de Autenticación. En este caso, los proveedores de servicios externos se conectan ellos mismos al servidor del Centro de Servicio de Autenticación para obtener de este centro los paquetes de datos de sus clientes y sus certificados respectivos.

El Centro de Servicio de Autenticación es la única entidad con capacidad de leer el código de autenticación digital (parte 2). A petición de un proveedor de servicios que desee comprobar los paquetes de datos enviados por sus clientes, el centro de servicio de autenticación comprueba si los datos “en texto en claro” (parte 1) y el código de autenticación digital son congruentes entre sí. Los datos de posicionamiento se considerarán “correctos” solamente si el Centro de Servicio de Autenticación puede garantizar que los datos de posicionamiento en cuestión han sido producidos por un receptor fiable e identificable y calculados mediante software reconocido y con licencia, basándose en señales de radionavegación seguras. Si la parte 1 y la parte 2 del paquete de datos coinciden, el Centro de Servicio de Autenticación proporciona al proveedor de servicios un certificado, el cual garantiza que los datos a proteger se integraron en el paquete de datos en el tiempo indicado y en la ubicación indicada. Si las dos partes no coinciden, el Centro de Servicio de Autenticación proporciona al solicitante un certificado que avisa que el paquete de datos no superó la prueba de autenticación (por ejemplo, debido a que los datos de posicionamiento o la identificación del receptor se han corrompido y, consecuentemente, el paquete de datos no se puede autenticar).

Un proveedor de servicios externo puede enviar al Centro de Servicio de Autenticación una solicitud de autenticación junto con el paquete de datos completo recibido por el proveedor de servicios desde uno de sus clientes. La autoridad de autenticación puede configurarse para interpretar la presentación de un paquete de datos como una solicitud de autenticación.

El Centro de Servicio de Autenticación descifra a continuación la Parte 2 (“la clave de autenticación”) y comprueba que la información contenida en la Parte 2 es congruente con la información contenida como texto en claro en la Parte 1.

Si los datos de las dos partes coinciden, el Centro de Servicio de Autenticación proporciona al solicitante un certificado, el cual certifica que el paquete de datos superó la comprobación de la congruencia y que por lo tanto se puede confiar en el mismo.

Si las dos partes no coinciden, el Centro de Servicio de Autenticación proporciona al solicitante un certificado que avisa que el paquete de datos no superó la comprobación de la congruencia y que consecuentemente, no se puede autenticar.

Procesado remoto de la autenticación de PVT

Si un proveedor de servicios o cualquier otro tercero está dispuesto a verificar la veracidad de la información contenida en la Parte 1 (“la información legible”) de un paquete de datos, el mismo tiene que dirigirse al Centro de Servicio de Autenticación.

En esta forma de realización de la invención, solo una autoridad en todo el mundo puede autenticar los paquetes de datos producidos por receptores. Con autenticación se pretende significar el envío, a cualquier solicitante, de un certificado que indica si la PVT, el ID Público de Receptor y, en su caso, el ID Público de Usuario, según se declaró en la Parte 1 “en texto en claro”, son correctos y qué nivel de confianza se puede conceder a esta información. La autoridad en cuestión es el Centro de Servicio de Autenticación.

El Centro de Servicio de Autenticación trata todas las solicitudes de certificados de autenticación que puede recibir a través de un software específico, denominado, en lo sucesivo en la presente, “software de autenticación”. Los solicitantes presentan solicitudes de certificados de autenticación junto con los correspondientes paquetes de datos a través de una red segura, denominada red de certificados (número de referencia 32 de la figura 1). La red de certificados se puede materializar a través del intercambio cifrado de datos por Internet.

El software de autenticación lee el ID Público de Receptor en la Parte 1. Este software tiene acceso a tres bases de

datos del Centro de Servicio de Autenticación:

- los archivos de todos los testigos criptográficos;
- la lista de todas las parejas de un ID Público de Receptor y un ID Secreto de Receptor.
- Una colección de las huellas (*footprints*) de todas las versiones de códigos de programa de receptores con licencia.

El Centro de Servicio de Autenticación gestiona y actualiza la segunda base de datos, en la que registra todas las parejas de ID Público de Receptor e ID Secreto de Receptor para la flota completa de receptores con licencia. El Centro de Servicio de Autenticación habría asignado parejas de ID Público de Receptor e ID Secreto de Receptor a fabricantes con licencia para la producción de receptores.

Etapa 1: comprobación de la Parte 1

En primera instancia el software de autenticación comprueba si la Parte 1 contiene tanto una PVT como un ID Público de Receptor en un formato correcto. Por ejemplo, si la Parte 1 ha sido cifrada por cualquier participante antes de ser presentada como adjunto a una solicitud de autenticación, la solicitud de autenticación se abortará. En particular, la Parte 1 debería estar en claro, es decir, no cifrada.

Si la PVT declarada y/o el ID Público de Receptor no está(n) en un formato correcto, el software de autenticación emite un certificado indicando que el proceso de autenticación no se puede llevar a cabo debido a una Parte 1 alterada.

Etapa 2: primer descifrado de la Parte 2

El software de autenticación recupera el ID Secreto de Receptor, sobre la base del ID Público de Receptor declarado en la Parte 1 (“la información legible”), del receptor que ha producido el Paquete de datos en cuestión.

El software de autenticación, a continuación, usa el ID Secreto de Receptor para descifrar la Parte 2 - o En2 - del paquete de datos. A continuación leerá En1 - todavía no utilizable ya que En1 está cifrado - y un patrón de 28 bits que identifica los satélites Galileo usados para el cálculo de la PVT.

Si el software de autenticación no puede descifrar la Parte 2 con el ID Secreto de Receptor, entonces el software de autenticación emitirá el certificado con una alerta que indica que o bien:

- el ID Público de Receptor ha sido alterado, lo cual significa que el ID Secreto de Receptor correspondiente no es la clave de descifrado correcta;
- o bien la Parte 2 (“el código de autenticación digital”) ha sido alterada y por lo tanto no se puede descifrar.

Un certificado con una alerta de este tipo implicará que la PVT declarada en la Parte 1 no se puede autenticar. A la inversa, no significa necesariamente que se ha suplantado la identidad de la PVT o que la misma se ha falsificado.

Si el software de autenticación puede descifrar la Parte 2 con el ID Secreto de Receptor, entonces el software de autenticación emitirá una información preliminar en el certificado indicando que el ID Público de Receptor declarado en la Parte 1 es correcto.

Etapa 3: Segundo descifrado de la Parte 2

Basándose en la lista de satélites Galileo declarados en el campo de identificador de vehículos espaciales de En2, el software de autenticación calcula la clave de descifrado para En1, gracias a los archivos de los testigos criptográficos de todos los satélites Galileo. Esta clave es una concatenación en un orden predeterminado de los testigos criptográficos recuperados sobre la base de la temporización proporcionada por la Parte 1 del paquete de datos (y, posiblemente, el ID Privado de Receptor).

Gracias a esta clave, el software de autenticación puede descifrar En1 y así acceder a todos los datos sucesivos calculados por el receptor:

- PVT_{E6},
- $PVT_{E1,E6}$,
- ID Público de Receptor,
- ID Público de Usuario (opcional),
- las dimensiones de la caja de PVT de confianza.

El software de autenticación lee todos los datos - contenidos en la Parte 2 en un formato cifrado - y los compara con los datos de la Parte 1 con el fin de comprobar si los dos conjuntos de datos son congruentes.

A tal efecto, el software de autenticación comprobará:

- si $PVT_{E1,E6}$ se corresponde con la PVT declarada en la Parte 1;
- si $PVT_{E1,E6}$ está contenida en la caja de PVT de confianza centrada en PVT_{E6}.
- si el ID Público de Usuario declarado opcionalmente en la Parte 1 coincide con el ID Público de Usuario contenido en la Parte 2.
- si el valor *hash* (huella digital) del software contenido en la Parte 2 se corresponde con una versión del software reconocida por el Centro de Servicio de Autenticación como fiable.

En función del resultado de estas comprobaciones, el software produce un certificado digital que indica si la PVT declarada es correcta y si es así, cuál es la precisión de confianza vinculada a la misma, y si el ID Público de Usuario declarado, en caso de que hubiera alguno, es correcto.

La razón para un cifrado de dos etapas y a continuación un descifrado de dos etapas está vinculada al hecho de que el software de autenticación no puede adivinar por adelantado qué satélites estaban bajo visibilidad del receptor en el momento del cálculo de PVT. En teoría, un cifrado y un descifrado podrían haber sido suficientes. De hecho, sobre la base de la temporización de la PVT declarada en la Parte 1 y de su posición en el globo, el software podría deducir cuáles eran entonces los 8 o menos satélites Galileo en el cielo por encima del receptor. Sin embargo, algunos de estos satélites podrían haber estado enmascarados y en consecuencia no detectados por el receptor. Con el fin de obtener la clave de descifrado correcta, el software tendría que llevar a cabo 2^8 pruebas con todas las concatenaciones posibles de testigos criptográficos, en correspondencia con la combinación de situaciones en las que se ha visto o no cada uno de los 8 satélites. Para evitar estos ensayos, que podrían retrasar el proceso de autenticación, el segundo cifrado y el primer descifrado correspondiente proporcionarán al software de autenticación la información correcta sobre qué satélites tienen que tenerse en cuenta para calcular la clave de descifrado con el fin de obtener acceso a la PVT encapsulada.

Etapa 4: transmisión al solicitante de un certificado de autenticación

El Centro de Servicio de Autenticación envía a continuación al solicitante el paquete de datos presentado, junto con un certificado que indica:

- Información 1: si la Parte 1 está en el formato correcto;
- Información 2: si es así, si el ID Público de Receptor declarado es correcto;
- Información 3: si es así, si la PVT declarada no ha sido manipulada indebidamente;
- Información 4: si es así, si el software a bordo del receptor de autenticación es reconocido por el Centro de Servicio de Autenticación;
- Información 5: si es así, si los mensajes de navegación en E1, E6B (y opcionalmente también E5A) son congruentes;
- Información 6: si es así, si la PVT declarada está contenida en la caja de PVT de confianza;
- Información 7: si el ID Público de Usuario declarado es correcto;
- Información 8: si es así, la precisión de “autenticación” medida en metros y basada en las dimensiones de la caja de PVT de confianza.

Las Informaciones 1 a 8 son datos booleanos. La Información 8 es un número entero. Estas informaciones indican lo siguiente:

- Si Información 1 es FALSA, entonces el certificado no tiene valor de ningún tipo y las otras Informaciones son irrelevantes.
- Si Información 2 es FALSA, entonces el certificado no tiene valor de ningún tipo y las otras Informaciones también son irrelevantes.
- Si Información 3 es FALSA, entonces el certificado demuestra que la PVT declarada en la Parte 1 se ha

modificado después de su cálculo en el receptor;

- Si Información 4 es FALSA, entonces el certificado demuestra que el software usado para calcular la PVT no es conocido para el Centro de Servicio de Autenticación;

- Si Información 5 es FALSA, entonces el certificado demuestra que el receptor ha sido supuestamente sometido a un ataque de suplantación de identidad en E1 aunque PVT_{E6} sigue siendo fiable;

- Si Información 6 es FALSA, entonces el certificado demuestra que lo más probable es que el receptor haya sido sometido a un ataque sobre las señales de radionavegación pero que PVT_{E6} sigue siendo fiable;

- Si Información 7 es FALSA, entonces el certificado demuestra que el ID Público de Usuario, si hay alguno, declarado en la Parte 1 no se ha modificado más que después de su cálculo en el receptor.

El certificado no proporciona la PVT o el ID Público de Receptor. En otras palabras, si la Parte 1 ("la información legible") se presenta de una manera cifrada o si está ausente, entonces el Centro de Servicio de Autenticación considera que el solicitante no ha sido autorizado por el usuario del receptor para obtener acceso a esta información. A continuación, el Centro de Servicio de Autenticación no revelará que ni la PVT ni el ID Público de Receptor. En otros términos, el servicio de autenticación no está destinado a vulnerar una protección de la privacidad - a pesar de que técnicamente podría hacerlo si la Parte 2 (el código de autenticación digital) no ha se ha vuelto cifrar.

La producción de certificados para paquetes de datos procedentes de todas partes del mundo posibilita indirectamente que el Centro de Servicio de Autenticación garantice una vigilancia a nivel mundial de las frecuencias de navegación, y por lo tanto que detecte y localice ataques por interferencias deliberadas, por suplantación de identidad y por retransmisión de señales falseadas. El Centro de Servicio de Autenticación por ejemplo podría alertar a las autoridades nacionales sobre los estados afectados por dichos ataques identificados.

Robustez frente a amenazas de GNSS

Robustez frente a interferencias deliberadas

La solicitud no puede proteger contra un ataque simultáneamente en todas las frecuencias de navegación. Sin embargo - si por lo menos una de las frecuencias de navegación no sufre interferencias deliberadas - el ataque por interferencias deliberadas será detectado y vencido, es decir que el receptor puede seguir confiando en la PVT obtenida a partir de la frecuencia en cuestión.

Robustez frente a la suplantación de identidad

Los dispositivos existentes para suplantación de identidad no pueden simular cualquier señal cifrada. En particular no pueden simular códigos de determinación de la distancia E6B del Galileo. Por lo tanto, los códigos E6B no son vulnerables a amenazas de suplantación de identidad.

Sin embargo, una primera adquisición directa en E6B es muy compleja debido al hecho de que el código de ensanchamiento E6B es secuencias criptográficas no periódicas. Una buena estimación del tiempo es obligatoria e implica que una primera adquisición de la señal se realiza en E1A. Esta primera estimación del tiempo permitirá iniciar el proceso de adquisición en E6B. Si el mensaje de navegación en E1A se manipula indebidamente (por suplantación de identidad) entonces la adquisición de E6B no se puede iniciar. Así, la primera contramedida es comprobar si se puede llevar a cabo la adquisición de E6B. En caso negativo, el receptor usa una señal comprometida de E1A.

Por otra parte, para calcular una PVT_{E6}, se requieren datos de navegación fiables (efemérides, correcciones de reloj, etcétera) en el mensaje de datos de E6B.

Por lo tanto, el receptor de autenticación comprueba la integridad de cada uno de los datos de navegación recibidos, mediante la comparación de la huella digital de los datos de navegación recibidos en la señal cifrada de E6B y el valor de SHA-256 de los datos de navegación recibidos en E1A (para todos los satélites Galileo usados para calcular una solución de PVT).

El testigo criptográfico pretende proporcionar un mecanismo de anti-reproducción frente a un ataque sobre el cifrado del código digital de autenticación.

El receptor de autenticación calculará dos soluciones de PVT (usando los mismos satélites Galileo). Sin embargo, aunque $PVT_{E1,\ E6}$ es la más precisa, solo PVT_{E6} es robusta frente a ataques de suplantación de identidad y es la referencia fiable que se usará para determinar el área de confianza (autenticación de SIS autónoma).

Robustez frente a la retransmisión de señales falseadas

La retransmisión de señales falseadas es los medios más eficaces para engañar a receptores GNSS. Ni siquiera los servicios denominados “robustos” tales como el código P(Y) GPS o el PRS del Galileo son inmunes a la retransmisión de señales falseadas.

No obstante, la retransmisión de señales falseadas se puede vencer en caso de que el atacante no retransmita señales falseadas para todo el espectro de frecuencias usadas con fines de navegación, es decir E1, E5 y E6. Un receptor de multi-frecuencia puede detectar entonces fácilmente incongruencias entre el posicionamiento proporcionado por PVT_{E1}, PVT_{E5} y PVT_{E6}. Esto será así para receptores según el presente ejemplo.

Pueden detectarse también algunos ataques de retransmisión de señales falseadas en los que un receptor detecta un salto repentino en la posición y/o en la temporización de la PVT calculada. Los receptores de autenticación integrarán esta función.

Los ataques de retransmisión de señales falseadas que ejercen una deriva progresiva del tiempo y/o la posición sobre los receptores pueden permanecer sin ser detectados si estos receptores se basan solamente en señales GNSS. Sin embargo, los ataques de este tipo pueden detectarse siempre que los receptores estén equipados también con sensores de navegación inercial. Receptores de autenticación incluirán sensores de este tipo.

Robustez frente a la posible alteración de datos de posicionamiento

La aplicación no puede evitar que un atacante modifique la PVT y/o el ID Público de Receptor en la Parte 1 del paquete de datos, especialmente si la información a proteger se almacena o transmite en texto en claro. Sin embargo, la aplicación servirá para detectar dicha alteración.

Para combatir la manipulación indebida de la PVT, el software del receptor puede incluir un algoritmo que posibilita que el usuario proteja el paquete de datos generado que se va a enviar a los proveedores de servicios y a los clanes del usuario. Este cifrado constituye unos buenos medios para la protección ante un intento, por parte de un tercero, de modificar en la Parte 1 del paquete de datos la PVT y/o el ID Público de Receptor.

Vulnerabilidades ante ataques en la propia aplicación

Todos los recursos de seguridad, incluyendo los microprogramas del receptor se implementan dentro del perímetro de seguridad del Receptor de autenticación. Además, el equipo anfitrión incluye mecanismos que permiten la comprobación de datos y de la integridad del software usados para calcular PVT.

El receptor GNSS dedicado estará equipado con un módulo criptográfico que evita que el software crítico y los recursos de seguridad sean leídos y por lo tanto robados (incluso por parte del usuario o del proveedor de servicios).

La amenaza en este caso es que un atacante produce paquetes de datos de confianza falsos, que superarán la “prueba del certificado” con éxito y que sin embargo han sido falsificados. Con el fin de vencer a la aplicación de autenticación, el atacante tendrá que:

(1) desentrañar un ID Privado de Receptor;
(2) archivar, durante el periodo de tiempo afectado por el ataque, todos los NONCEs y todas las efemérides; y
(3) dilucidar la ingeniería inversa del software de encapsulamiento.

La acción (1) será muy difícil de lograr. Requerirá la obtención de un acceso no autorizado a la base de datos de ID de Receptor del Centro de Servicio de Autenticación o la lectura del contenido de la memoria a prueba de manipulaciones indebidas del Receptor de autenticación. O alternativamente, el ID Privado de Receptor se puede desentrañar mediante “ataques de fuerza bruta”, aunque los únicos datos cifrados con el ID Privado de Receptor tienen una longitud de solamente 28 bits. Los algoritmos del estado de la técnica actual ya son inmunes a ataques de fuerza bruta con el poder computacional de los ordenadores actuales. La breve longitud de los datos cifrados haría que resultase todavía más difícil para un atacante desentrañar la clave en el futuro. Otra amenaza es que el fabricante mantenga un rastro de la relación entre el ID Público de Receptor y el ID Privado de Receptor y que este rastro sea robado: debe obligarse a los fabricantes a destruir dicha información después de la producción de los receptores de autenticación.

La acción (2) solamente es posible si el atacante tiene acceso a las claves de navegación durante un período de tiempo prolongado y puede archivar todos los NONCEs identificados en el mensaje de datos E6B. La acción (2) debería evitarse:

- imponiendo un perímetro de seguridad en todos los receptores de CS (la primera etapa es no hacer público el Documento de Control de la Interfaz del Servicio Comercial y permitir la construcción de receptores del Servicio Comercial solamente a fabricantes con licencia);

- establecer estándares altos de perímetro de seguridad de receptores de autenticación;
- proteger la distribución de las claves de navegación.

La acción (3) puede lograrse en primer lugar robando software de encapsulamiento con licencia. La distribución y actualización de este software debe garantizarse a través de canales protegidos. La ingeniería inversa se evitará de una manera satisfactoria mediante una actualización regular y frecuente de los testigos criptográficos.

Ninguna de estas acciones está al alcance de ningún pirata informático tomando como base las mejores tecnologías actuales.

REIVINDICACIONES

1. Procedimiento para proporcionar una indicación de tiempo-y-ubicación autenticable usando un receptor de señales de radionavegación, comprendiendo dicho procedimiento las siguientes etapas:

a) recibir señales de radionavegación difundidas desde una pluralidad de fuentes de señales de radionavegación, conteniendo por lo menos algunas de dichas señales de radionavegación uno o más testigos criptográficos protegidos mediante cifrado, actualizándose de vez en cuando dichos testigos criptográficos;

b) recuperar dichos testigos criptográficos a partir de dichas señales de radionavegación que los contienen, mediante descifrado;

c) determinar datos de posicionamiento basándose en dichas señales de radionavegación recibidas, incluyendo dichos datos de posicionamiento, la posición geográfica y el tiempo de dicho receptor de señales de radionavegación;

d) generar un código de autenticación digital usando una función criptográfica que toma como entradas por lo menos dichos datos de posicionamiento y dichos testigos criptográficos recuperados; y

e) producir un paquete de datos que incluye una primera y una segunda partes, de manera que dicha primera parte contiene dichos datos de posicionamiento y un identificador público de receptor y dicha segunda parte contiene dicho código de autenticación digital.

2. Procedimiento según la reivindicación 1, en el que cada una de dichas señales de radionavegación que contiene un testigo criptográfico contiene un testigo criptográfico específico de la fuente de señales de radionavegación que difunde dicha señal de radionavegación.

3. Procedimiento según la reivindicación 2, en el que dicha primera parte o dicha segunda parte contiene además datos de identificación de fuentes que identifican las fuentes de señales de radionavegación que han difundido las señales de radionavegación a partir de las cuales se han recuperado dichos testigos criptográficos.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que dicha función criptográfica produce, en calidad de dicho código de autenticación digital, un valor *hash* o un texto cifrado de por lo menos dichos datos de posicionamiento, sobre la base de una clave criptográfica que es una función de por lo menos dichos testigos criptográficos recuperados.

5. Procedimiento según la reivindicación 4, en el que dicha función criptográfica produce dicho valor *hash* o texto cifrado de por lo menos dichos datos de posicionamiento y dicho identificador público de receptor.

6. Procedimiento según las reivindicaciones 4 o 5, que comprende proporcionar datos adicionales a proteger, tales como, por ejemplo, datos de identificación de usuario, datos de integridad de la señal-en-el-espacio, una huella digital de software del receptor, datos de posicionamiento adicionales, firma digital que identifica al usuario y/o uno o más documentos digitales, en el que dicho código de autenticación digital se genera usando dicha función criptográfica que toma como entrada también dichos datos adicionales a proteger.

7. Procedimiento según la reivindicación 6, en el que dicha función criptográfica produce un valor *hash* o un texto cifrado de por lo menos dichos datos adicionales a proteger sobre la base de dicha clave criptográfica.

8. Procedimiento según una cualquiera de las reivindicaciones 4 a 7 en combinación con la reivindicación 2, en el que dicha clave criptográfica comprende una concatenación de dichos testigos criptográficos.

9. Procedimiento según la reivindicación 8, en el que dicho receptor ha almacenado en el mismo un identificador secreto de receptor conocido para dicha autoridad de autenticación y en el que dicha clave criptográfica comprende una concatenación de dichos testigos criptográficos y parte o la totalidad de dicho identificador secreto de receptor.

10. Procedimiento según cualquiera de las reivindicaciones 1 a 8, que comprende cifrar dicha segunda parte, por ejemplo, de acuerdo con un esquema de cifrado simétrico.

11. Procedimiento según cualquiera de las reivindicaciones 1 a 10, en el que las correspondientes de dichas señales de radionavegación que contienen un testigo criptográfico son señales de radionavegación cifradas y/o contienen dicho testigo criptográfico como parte de un contenido de datos cifrados.

12. Procedimiento según cualquiera de las reivindicaciones 1 a 11, que comprende solicitar de dicha autoridad de autenticación claves de navegación para acceder a dicho o dichos testigos criptográficos protegidos mediante cifrado y recibir dichas claves de navegación por medio de un canal de comunicaciones seguro.

13. Procedimiento según cualquiera de las reivindicaciones 1 a 12, en el que dicho receptor de señales de radionavegación comprende un perímetro de seguridad dentro del cual se llevan a cabo parte o la totalidad de las etapas a) a e).

14. Receptor de señales de radionavegación configurado para llevar a cabo el procedimiento según cualquiera de las reivindicaciones 1 a 13.

15. Procedimiento de comprobación de la autenticidad de un paquete de datos, comprendiendo dicho procedimiento:

recibir un paquete de datos que ha sido producido supuestamente de acuerdo con el procedimiento según cualquiera de las reivindicaciones 1 a 13, incluyendo dicho paquete de datos una primera parte que contiene datos de posicionamiento y una segunda parte que contiene un código de autenticación digital, incluyendo dichos datos de posicionamiento posición geográfica y tiempo supuestos;

recuperar uno o más testigos criptográficos que habría recibido un receptor de señales de radionavegación si el mismo hubiese estado realmente en dicha posición geográfica en dicho tiempo;

comprobar si dichos datos de posicionamiento y dicho código de autenticación digital son congruentes entre sí;

autenticar dicho paquete de datos si dichos datos de posicionamiento y dicho código de autenticación digital son congruentes entre sí, o rechazar dicho paquete de datos como no válido si dichos datos de posicionamiento y dicho código de autenticación digital no son congruentes entre sí.

Fig. 1

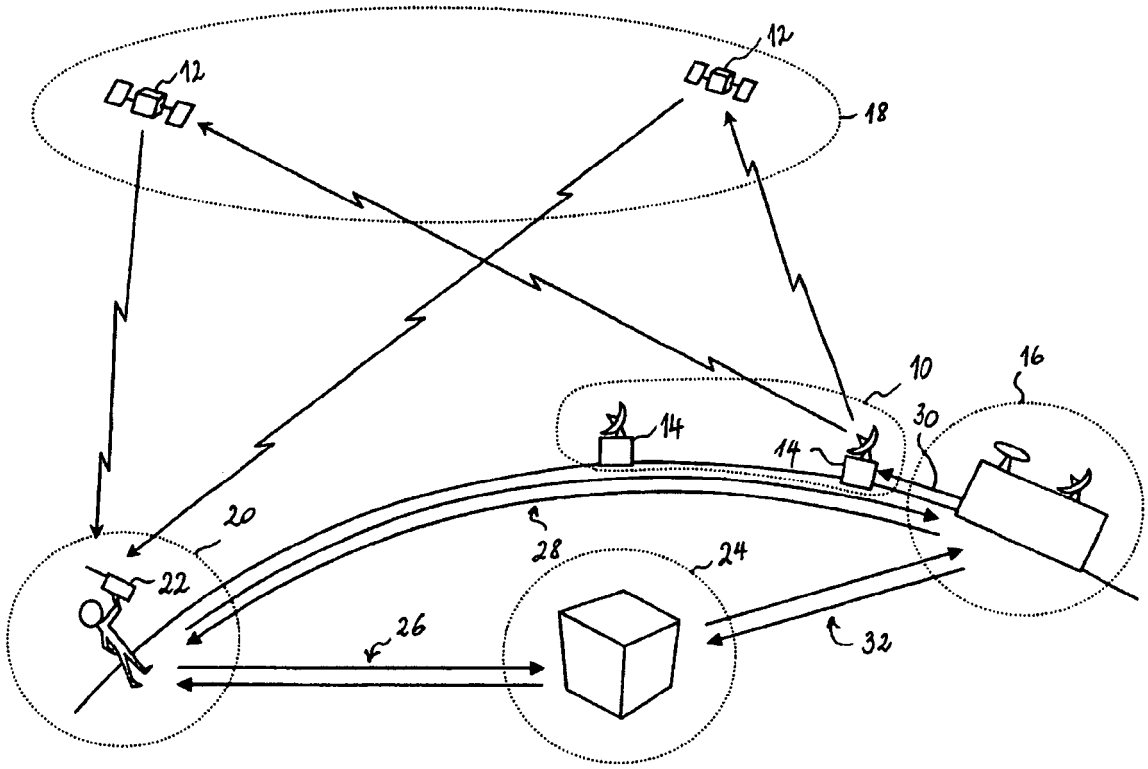


Fig. 2

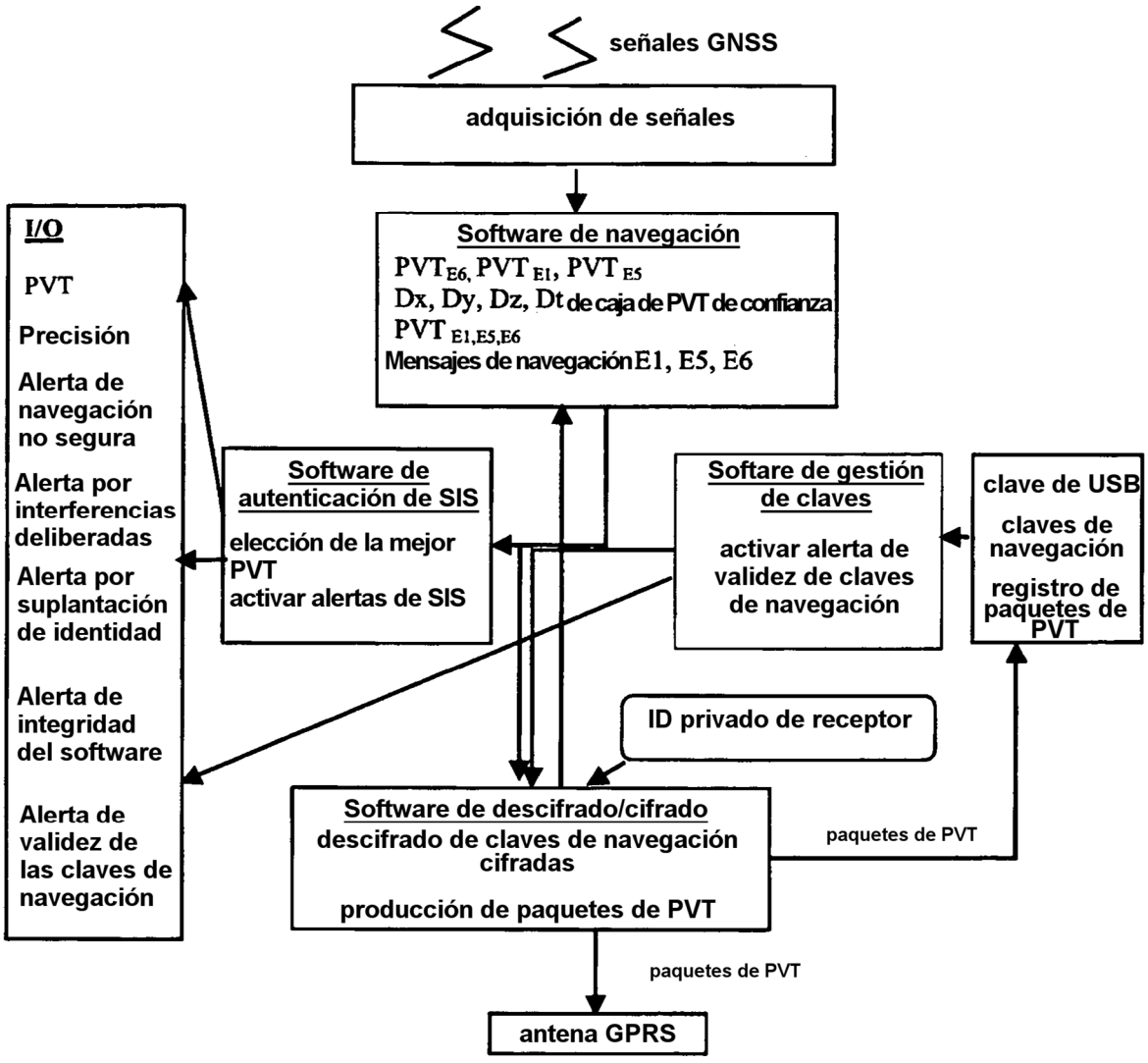

señales GNSS
adquisición de señales
Software de navegación
PVT E6, PVT E1, PVT E5
Dx, Dy, Dz, Dt de caja de PVT de confianza
PVT E1,E5,E6
Mensajes de navegación E1, E5, E6
I/O
PVT
Precisión
Alerta de navegación no segura
Alerta por interferencias deliberadas
Alerta por suplantación de identidad
Alerta de integridad del software
Alerta de validez de las claves de navegación
Software de autenticación de SIS
elección de la mejor PVT
activar alertas de SIS
Softare de gestión de claves
activar alerta de validez de claves de navegación
clave de USB
claves de navegación
registro de paquetes de PVT
ID privado de receptor
Software de descifrado/cifrado
descifrado de claves de navegación cifradas
producción de paquetes de PVT
paquetes de PVT
paquetes de PVT
antena GPRS

Fig. 3

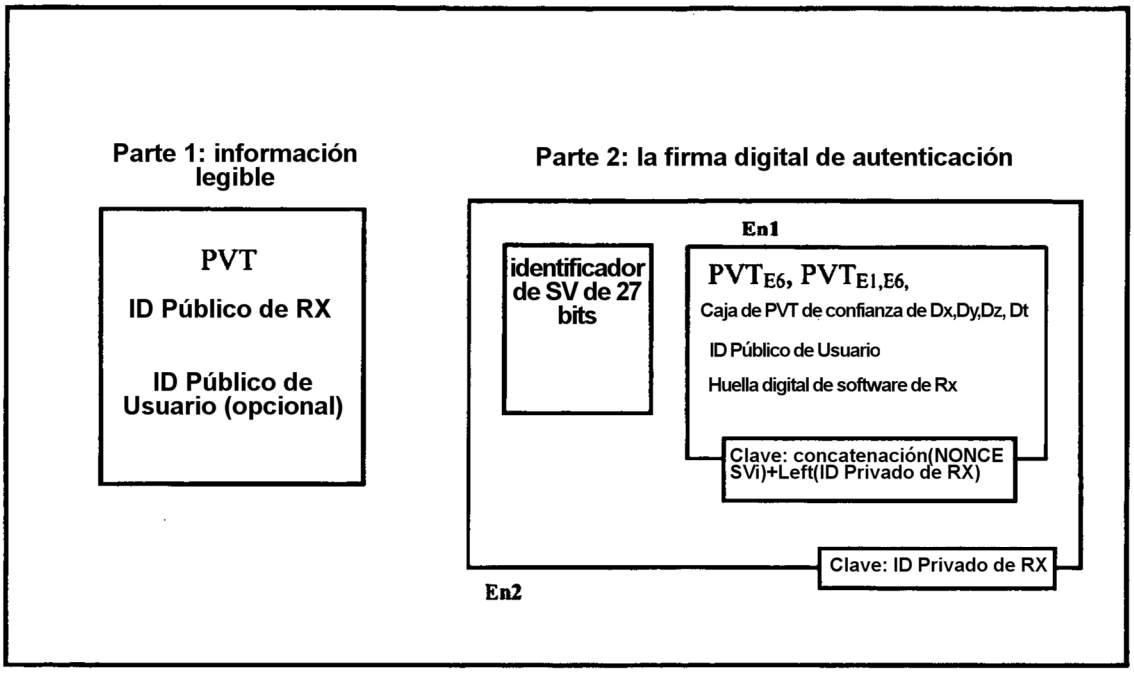
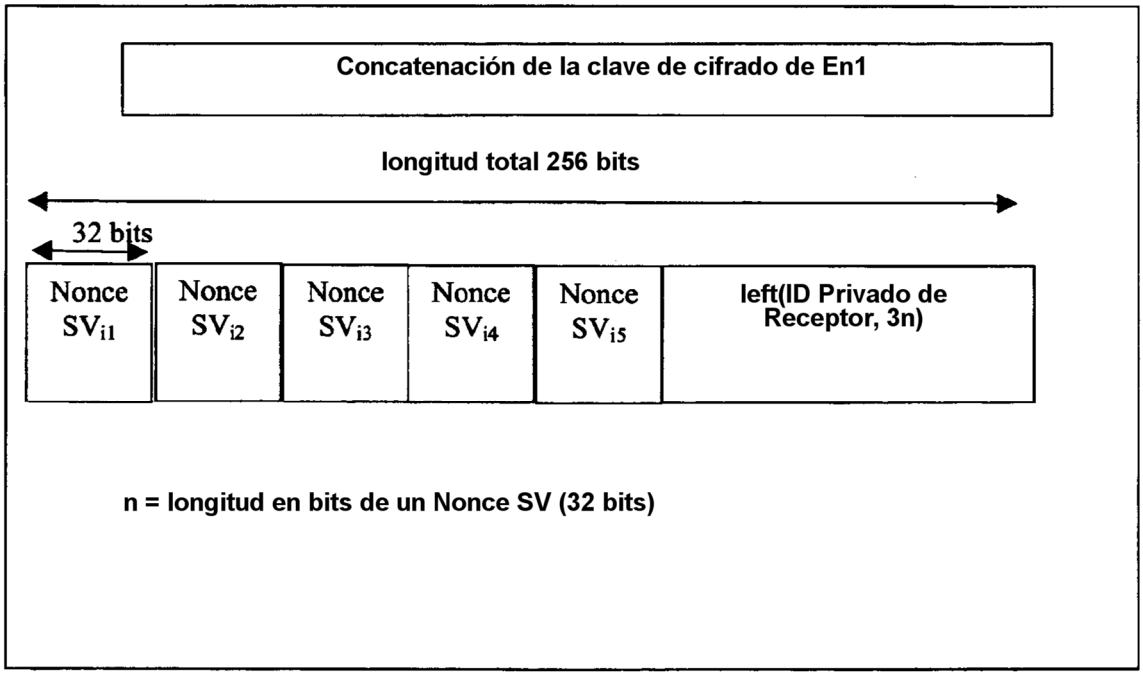

Parte 1: información legible
PVT
ID Público de RX
ID Público de Usuario (opcional)
Parte 2: la firma digital de autenticación
En1
identificador de SV de 27 bits
PVTE6, PVTE1,E6,
Caja de PVT de confianza de Dx,Dy,Dz, Dt
ID Público de Usuario
Huella digital de software de Rx
Clave: concatenación(NONCE SVi)+Left(ID Privado de RX)
Clave: ID Privado de RX
En2

Fig. 4


Concatenación de la clave de cifrado de En1
longitud total 256 bits
32 bits
Nonce SVi1
Nonce SVi2
Nonce SVi3
Nonce SVi4
Nonce SVi5
left(ID Privado de Receptor, 3n)
n = longitud en bits de un Nonce SV (32 bits)