(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 895 116**

(51) Int. CI.:

H04W 12/04 (2011.01)
H04W 12/069 (2011.01)
H04W 4/44 (2008.01)
H04W 12/02 (2009.01)
H04W 12/75 (2011.01)
H04W 12/40 (2011.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2016 PCT/US2016/067261**

(87) Fecha y número de publicación internacional: **22.06.2017 WO17106705**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2016 E 16840358 (2)**

(97) Fecha y número de publicación de la concesión europea: **06.10.2021 EP 3391681**

(54) Título: **Sistema de comunicación segura para vehículos**

(30) Prioridad:

17.12.2015 US 201562268834 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2022

(73) Titular/es:

ONBOARD SECURITY, INC. (100.0%)
5775 Morehouse Drive
San Diego, CA 92121, US

(72) Inventor/es:

ETZEL, MARK, HOWARD;
COLEMAN, JAMES, PATRICK;
SAVINA, CHRISTOPHER, LEE y
COX, MICHAEL, TWOMEY

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistema de comunicación segura para vehículos

La presente invención se refiere a un sistema de comunicación segura para vehículos que comprende almacenar credenciales durante una vida útil prevista de un vehículo o una parte significativa de la vida útil prevista del vehículo en archivos de credenciales en un almacén en un vehículo, en el que cada credencial incluye una clave privada de firma y un certificado digital y es válida durante un marco de tiempo específico, almacenar un índice en los archivos de credenciales en el almacén del vehículo, en el que el índice indexa el archivo de credenciales durante los marcos de tiempo en los que son válidas las credenciales almacenadas en los archivos de credenciales, utilizar el índice para recuperar los archivos de credenciales durante un periodo, en el que las credenciales en los archivos de credenciales recuperados son válidas durante el periodo, y utilizar al menos uno de los archivos de credenciales recuperados para su uso en el sistema de comunicaciones del vehículo durante el periodo.

El documento XP002555811 da a conocer la colocación de un índice de número entero dentro de un nombre de archivo de archivos de credenciales de certificado de clave pública para identificar rápidamente certificados válidos de clave pública almacenados en dichos archivos. El documento XP013145534 da a conocer la colocación del periodo de tiempo de validez dentro de un nombre de archivo de los archivos de credenciales de certificado de clave pública para identificar rápidamente los certificados válidos de clave pública almacenados en dichos archivos.

ESTADO DE LA TÉCNICA ANTERIOR

Se han presentado numerosas propuestas para proporcionar comunicaciones inalámbricas entre vehículos y entre un vehículo y unidades a pie de carretera. Los ejemplos de dichas propuestas incluyen el conjunto de estándares IEEE 1609 para acceso inalámbrico en entornos de vehículos (WAVE) y los estándares ETSI para sistemas de transportes inteligentes. En estos sistemas, las comunicaciones pueden ayudar a mejorar la seguridad de los vehículos, a proporcionar información adicional y a proporcionar servicios adicionales. Por ejemplo, las comunicaciones pueden ayudar a evitar colisiones, proporcionar avisos de colisión, mejorar el flujo de tráfico, proporcionar orientación de navegación y ruta, proporcionar información de puntos de interés y proporcionar diagnósticos remotos. También se han propuesto muchos otros usos de estas comunicaciones.

La Fig. 1 representa un diagrama de un sistema ejemplar 100 en el que los vehículos pueden comunicarse inalámbricamente entre sí y con diversos componentes fuera del camino. Los vehículos 102, 104 y 106 están situados en una calzada y pueden comunicarse inalámbricamente entre sí según se indica mediante las flechas en la Fig. 1. Los vehículos 102, 104 y 106 también pueden comunicarse inalámbricamente con las unidades a pie de carretera 110 y 112. El vehículo 106 puede comunicarse inalámbricamente con una unidad interconectada con una red telefónica inalámbrica 120. La red telefónica inalámbrica puede incluir una conexión a una red 122, tal como Internet, en la que varios servidores pueden proporcionar servicios. Las unidades a pie de carretera 110 y 112 también pueden conectarse a la red 122 mediante una puerta de enlace 114.

SUMARIO

Según la presente invención, se proporciona un método en un sistema de comunicación segura para vehículos, según se define en la reivindicación independiente 1. La invención se define además mediante la reivindicación independiente 5.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1 muestra un ejemplo de un sistema de comunicaciones del vehículo.

La FIG. 2 muestra componentes en una infraestructura de clave pública (PKI) ejemplar que están implicados en la concesión de un certificado digital.

La FIG. 3 muestra componentes en un ecosistema de comunicaciones del vehículo implicado en la validación de una comunicación firmadas con componentes.

La FIG. 4 representa un número de componentes que pueden encontrarse en un certificado digital en realizaciones ejemplares.

La FIG. 5 representa algunos de los componentes encontrados en una credencial en realizaciones ejemplares.

La FIG. 6 representa un archivo de índice y archivos de credenciales que contienen credenciales que están indexadas mediante el archivo de índice.

La FIG. 7 es un diagrama de flujo que ilustra etapas que se realizan para acceder a archivos de credenciales precargados.

La FIG. 8 es un diagrama de flujo que ilustra etapas que se realizan para prederivar claves.

La FIG. 9 es un diagrama de flujo que ilustra etapas que se realizan para llevar a cabo un cambio de identidad.

La FIG. 10 es un diagrama de flujo que ilustra el uso de una API en realizaciones ejemplares.

La FIG. 11 representa una unidad de abordo y diversas unidades de aplicación en un vehículo en realizaciones ejemplares.

La FIG. 12 representa componentes ejemplares que pueden encontrarse en una unidad de abordo en realizaciones ejemplares.

La FIG. 13 ilustra un número de posibilidades diferentes para una lógica de procesamiento 1300 para la lógica de procesamiento en realizaciones ejemplares.

La FIG. 14 ilustra interacciones entre aplicaciones y funcionalidades protegidas en realizaciones ejemplares.

DESCRIPCIÓN DETALLADA

Las realizaciones ejemplares del presente documento se refieren a proporcionar seguridad y privacidad en un sistema de comunicación segura para vehículos, tal como los discutidos en el estado de la técnica anterior en relación a la FIG. 1. El sistema de comunicación segura para vehículos proporcionado por las realizaciones ejemplares puede conformarse con el estándar IEEE 1609.2-2016 y los estándares ETSI TS103097 y TS102941. El sistema de comunicación segura para vehículos también puede conformarse con un perfil del sistema básico del Consorcio de comunicaciones Car2Car.

Los servicios de seguridad proporcionados por la realización ejemplar pueden ser realizados en gran parte por una biblioteca de módulos, tal como módulos de biblioteca de enlaces dinámicos. Las realizaciones ejemplares pueden implementar un sistema integrado que contiene la lógica de procesamiento, el almacén y el software para realizar la funcionalidad deseada. El sistema integrado puede residir en un vehículo o en una unidad a pie de carretera. El sistema integrado puede incluir un hardware seguro para mantener claves privadas y realizar claves privadas en las claves privadas.

Las realizaciones ejemplares descritas en el presente documento proporcionan un número de optimizaciones y mejoras que proporcionan una mejor seguridad y rendimiento para dicho sistema de comunicación segura para vehículos.

Los mensajes en el sistema de comunicación segura para vehículos deben estar protegidos frente a ataques, tal como escuchas, suplantación de identidad, alteración y reproducción. Además, debe protegerse la privacidad de las partes implicadas en el sistema de comunicaciones seguras. La información personal, la información de identificación y la información enlazable no deben filtrarse a partes no autorizadas.

La seguridad proporcionada por el sistema de comunicación segura para vehículos puede depender de una infraestructura de clave pública (PKI). La PKI gestiona certificados digitales y encriptación de clave pública. Una clave está vinculada a una parte a través de un proceso de emitido como certificados por una autoridad de certificación (AC). La FIG. 2 representa interacciones de una parte 200 para obtener un certificado digital 210 en un sistema de comunicaciones de vehículos basado en EE.UU. ejemplar. El proceso comienza con una parte 200 que somete una petición 202 a una autoridad de registro 204. La petición 202 puede incluir una clave pública. La autoridad de registro 204 confirma que la parte es un dispositivo válido en el sistema para la autoridad de certificación 208 en forma de una aprobación 206. La autoridad de certificación 208 emite entonces un certificado digital 210 que se pasa a la autoridad de registro 204 y se devuelve a la parte 200. El certificado digital demuestra la propiedad de la clave pública. En el sistema de comunicación segura para vehículos, el certificado digital es un documento firmado digitalmente que vincula la clave pública a una identidad y/o un conjunto de permisos. El flujo y partes implicados en un sistema de comunicaciones de vehículos basado en Europa pueden ser diferentes. La descripción de la Fig. 2 está destinado a ser meramente ejemplar y no limitante.

Como se muestra en la FIG. 3, una vez que una parte ha recibido un certificado digital, la parte puede usar el certificado digital en comunicaciones. La FIG. 3 muestra el caso en el que una primera parte 300 firma digitalmente una comunicación 302 para ser enviada a una segunda parte 304 con una clave privada. La segunda parte 304 verifica entonces la firma en la comunicación firmada 302 usando la clave pública de la primera parte y valida la identidad de la primera parte 300 validando un certificado digital que vincula la clave pública a la primera parte 300. Esta validación puede implicar enviar una petición de validación 306 al componente de la autoridad de validación 308 que devuelve una validación 312. La autoridad de validación 308 probablemente es parte o está presente en la segunda parte 304

y no un componente separado. El componente de validación 308 puede basarse en información de una autoridad de certificación 310 para validar la identidad.

La FIG. 4 muestra un ejemplo de un certificado digital 400. El certificado digital puede incluir numerosos tipos de información almacenados en diversos campos. El certificado digital 400 puede incluir información sobre una clave 404. Como se ha mencionado anteriormente, el certificado vincula la identidad de una parte o los permisos para la clave. Esta información puede incluir la clave real o puede incluir información que puede utilizarse para derivar la clave u obtener de otro modo la clave. El certificado digital puede incluir una firma digital 408 que se crea usando una clave privada de firma. Pueden usarse numerosos algoritmos diferentes para generar la firma digital.

Debido a que los certificados digitales son válidos únicamente durante periodos de tiempo específicos, el certificado digital 400 puede incluir un momento de inicio 410 y un momento de finalización 412. Como alternativa, pueden proporcionarse un momento de inicio y un valor de duración u otra información que identifique el periodo en el que el certificado digital es válido. Los certificados digitales expiran para proporcionar una seguridad mejorada para que una parte que supervisa el flujo de certificados digitales no pueda comprometer el sistema. Por último, el certificado digital puede incluir una información de ubicación geográfica 414. El certificado puede incluir numerosos permisos 416. Por ejemplo, los permisos 416 pueden especificar el tipo de mensajes con los que se usa el certificado. Los permisos 416 pueden especificar qué tipo de certificados pueden emitirse a partir del certificado. También pueden especificarse otros permisos.

Los expertos en la técnica apreciarán que la representación del certificado digital en la Fig. 4 está destinado a ser meramente ilustrativo y no limitante. Los certificados digitales pueden contener un conjunto diferente de campos que los que se muestran en la Fig. 4 en algunas realizaciones.

Un certificado es un "certificado explícito" si la clave pública es dada explícitamente en el certificado. Por el contrario, un certificado es un certificado implícito si no contiene la clave pero en su lugar contiene información en forma de un valor de reconstrucción que puede usarse junto con la clave pública y el certificado del usuario para reconstruir la clave de verificación utilizando una función de reconstrucción. Un certificado implícito no contiene ninguna firma.

El sistema de comunicación segura para vehículos de las realizaciones ejemplares pueden utilizar cadenas de certificados. En una cadena de certificados, los certificados se ordenan de arriba hacia abajo de modo que cada certificado en la cadena es el "certificado emisor" del que está debajo y es el "certificado subordinado" para el certificado que está por encima.

Un primer certificado es el certificado emisor para un segundo certificado si el titular del primer certificado usó la clave privada del primer certificado para crear la forma final del segundo certificado, ya sea firmándolo en el caso de un certificado explícito como creando un valor de reconstrucción en el caso de un certificado implícito. La contraparte de un certificado emisor es un certificado subordinado.

Las realizaciones ejemplares descritas en el presente documento pueden emplear la noción de credencial. Como se muestra en la FIG. 5, una credencial 500 incluye una clave privada de firma 502 y un certificado digital 504.

Las credenciales se utilizan para asegurar las comunicaciones en el sistema de comunicaciones seguras de las realizaciones ejemplares. La clave privada de firma se utiliza para firmar comunicaciones digitalmente, y los certificados se utilizan para vincular una clave pública a una identidad y/o a un conjunto de permisos. Un certificado certifica que una clave pública es auténtica para un dispositivo en el sistema.

Puede haber presentes en el sistema uno o más administradores locales de certificados (LCM) para administrar los cambios de identidad y los certificados utilizados para firmas digitales. El LCM selecciona y proporciona el certificado correcto para firmar un mensaje saliente.

Cada aplicación puede abrir un contexto de seguridad. El contexto de seguridad elige uno o más LCM que pueden usarse para la aplicación. El contexto de seguridad define las propiedades de seguridad para la aplicación.

En realizaciones ejemplares, hay disponibles múltiples credenciales y son válidas durante una ventana de tiempo especificada. Por ejemplo, las credenciales pueden ser válidas durante un periodo de una semana para algunos conjuntos de credenciales. Los expertos en la materia apreciarán que el periodo de validez de las credenciales puede variar. En las realizaciones ejemplares, las credenciales que son válidas durante una ventana de tiempo especificada pueden almacenarse dentro de un archivo común, y estos archivos pueden indexarse mediante un índice clasificable. Como se muestra en la FIG. 6, los archivos de credenciales 600, 602 y 604 contienen las respectivas credenciales. Por ejemplo, el archivo de credenciales 600 contiene la credencial 606. Estos archivos de credenciales se indexan mediante un archivo de índice 608. El índice ayuda a localizar rápidamente las credenciales que son necesarias durante un periodo de tiempo específico. Cada uno de los archivos de credenciales 600, 602 y 604 tiene un nombre que incluye un momento de inicio en el cual son válidas las credenciales almacenadas en el archivo y estos nombres se utilizan para clasificar los archivos de credenciales y generar los archivos de índices clasificados 608 como se describirá con mayor detalle más adelante.

Algunas realizaciones ejemplares pueden utilizar un formato de archivo de credenciales designado como el formado de archivo de credenciales Aerolink (ACF, del inglés *Aerolink Credential File*). Los detalles de este formato de archivos se exponen más adelante.

El formato ACF proporciona un formato estándar de credenciales para uso interno dentro del sistema de comunicación segura para vehículos. El formato único es coherente y fácil de usar internamente. La información de credenciales puede ser recibida inicialmente en un formato diferente pero se almacena internamente en el formato ACF.

La credencial para una clave privada puede no estar predeterminada. La credencial para la clave privada puede residir tanto en el ACF como en un módulo de seguridad de hardware (HSM). Cada credencial puede usar datos para calcular su clave privada asociada dada una base común, por ejemplo, usando una clave de firma de oruga común a todas las credenciales, índices de mariposa y/o valores de reconstrucción privados por credencial.

Un valor semilla para generar la clave privada puede proporcionarse en el ACF o puede residir en un HSM. Un par de clave pública/privada puede utilizarse como una entrada para generar otro par de clave pública/privada. Por ejemplo, cuando se genera una petición para un certificado implícito, puede usarse una clave de semilla para derivar la clave pública final. En el modelo de claves de mariposa, por ejemplo, la clave de semilla puede expandirse en una clave de encriptación y/o en una clave de firma intermedia utilizando una función de expansión. Sin embargo, el propio ACF puede no estar encriptado.

Al utilizar el ACF, pueden permitirse uno o más periodos de validez en un solo archivo. Además, el formato de ACF puede permitir uno o más certificados por periodo de validez. El formato de ACF puede permitir una clave privada real, una referencia a una clave privada y/o datos para calcular una clave privada. El formato de ACF puede permitir diferentes tipos de referencias de clave privada. El formato de ACF puede permitir el acceso a las credenciales para cualquier momento de inicio especificado.

Los certificados y las claves agrupados en el formato de ACF pueden tener el mismo periodo de validez. Los certificados y las claves agrupados en el formato de ACF pueden tener los mismos tipos y números de claves privadas. Como resultado, estas condiciones pueden simplificar la implementación y pueden simplificar la búsqueda para un archivo al tener un tamaño de registro fijo.

El formato de ACF puede tener un nombre de archivo con un prefijo de uno o más caracteres seguidos de un guion. El formato de ACF puede tener un nombre de archivo con una extensión "acf". El formato de ACF puede tener, tras el prefijo, la fecha del momento de inicio más temprano de cualquier certificado en el archivo, expresado como AAAAMMDD, donde AAAA es el año de 4 dígitos, MM es el mes de 2 dígitos y DD es el día de 2 dígitos del mes. Por ejemplo, 20140616 puede representar el 16 de junio de 2014.

Cada ACF puede representar sus credenciales utilizando información contenida en un encabezado y/o información única y/o información individual contenida en un conjunto de registros, en el que puede haber un registro por credencial.

El encabezado para el formato ACF puede contener una cadena de caracteres que lo identifica como un archivo ACF. El encabezado para el formato ACF puede contener un número de versión del formato ACF. El encabezado para el formato ACF puede contener un indicador del protocolo del mensaje de que el contenido sigue, por ejemplo, un protocolo de mensaje IEEE o ETSI. El encabezado para el formato ACF puede contener un tipo de clave de firma, por ejemplo, un texto plano o índice en el HSM. El encabezado para el formato ACF puede contener la longitud de los índices de mariposa en cada registro. La longitud puede ser 0 y/o 1 si solo está presente un elemento de datos, por ejemplo, el elemento j, o 3 si están presentes dos elementos de datos, por ejemplo, los elementos en la posición j y en la posición i.

El encabezado para el formato ACF puede contener la longitud del valor de reconstrucción privado en cada registro. El encabezado para el formato ACF puede contener la longitud de la información de clave de firma en cada registro. El encabezado para el formato ACF puede contener el tipo de clave de desencriptación. El encabezado para el formato ACF puede contener la longitud de la información del registro de desencriptación en cada registro. El encabezado para el formato ACF puede contener la longitud del certificado en cada registro. El encabezado para el formato ACF puede contener el momento de inicio más temprano de cualquier registro. El momento de inicio para cada registro puede caer durante el día especificado en el nombre del archivo.

El encabezado para el formato ACF puede contener el intervalo de tiempo en segundos entre tiempos de inicio consecutivos de certificados o grupos de certificados, por ejemplo, el periodo de un registro que no incluye ningún periodo de solapamiento. Sin embargo, el intervalo de tiempo, no puede ser de 0 segundos. Si solo hay un certificado o grupo, el intervalo de tiempo puede ser la duración del certificado.

El encabezado para el formato ACF puede contener el número de registros que son válidos simultáneamente. Los registros pueden compartir el mismo momento de inicio. El encabezado para el formato ACF puede contener el número

de registros en el archivo. El encabezado para el formato ACF puede contener la longitud de la información de clave de firma de oruga.

El encabezado para el formato ACF puede contener la información de clave de firma de oruga. La información de clave de firma de oruga puede no estar presente si la longitud de la información de clave de firma de oruga es cero. El encabezado para el formato ACF puede contener la longitud de la clave estándar de encriptación avanzada (AES) para la ampliación de la clave de firma de oruga. El encabezado para el formato ACF puede contener la clave AES para la ampliación de la clave de firma de oruga. La clave AES puede no estar presente si la longitud de la clave AES para la longitud de ampliación de la clave de firma de oruga es cero.

La numeración de la versión de formato puede empezar por 1. Para cada revisión que dé como resultado una versión no retrocompatible, la versión de formato puede incrementarse.

Si no hay presente una clave de firma, puede indicarse el tipo de clave de firma. Si la clave de firma no está presente, la longitud de la clave de firma puede ser 0. Si no hay presente una clave de desencriptación, puede indicarse el tipo de clave de desencriptación. Si la clave de desencriptación no está presente, la longitud de la clave de desencriptación puede ser 0.

Un ACF puede contener, tras el encabezado del ACF, el número de registros indicados en el encabezado. Un ACF puede contener al menos un registro. Los registros en un ACF pueden ordenarse por tiempos ascendentes de inicio del certificado, comenzando con el primer momento de inicio indicado en el encabezado. Cada registro en un ACF puede contener un certificado e información para al menos una clave privada, por ejemplo, la propia clave, una referencia a la clave y/o información para calcular la clave. Cada registro en un ACF puede contener los mismos tipos y número de claves privadas. Cada registro en un ACF puede tener el certificado del mismo tamaño. Cada registro en un ACF puede tener la misma duración de validez. La duración de la validez puede especificarse en los campos del certificado.

Cuando se utiliza una pluralidad de ACF para contener los registros, que en total pueden extenderse varios días, los registros que son válidos al mismo tiempo, pero que excluyen cualquier periodo de solapamiento, pueden existir en el mismo archivo. Cada ACF puede comenzar con el encabezado de ACF con los campos ordenados.

El ACF puede utilizar una estructura de archivos específica. Las estructuras de archivos pueden ser una representación para listar y ordenar los campos en el ACF, pero únicamente los bytes de los campos están en el ACF. Como resultado, el ACF no contiene ningún relleno u otra información adicional.

El tipo de protocolo de mensaje para el ACF puede representarse de la siguiente manera:

```
typedef uint8_t MsgProtocol;
MsgProtocol const IEEE16092_D9_3 = 0;
Msg Protocol const ETSI103097_v1_1_1 = 1;
MsgProtocol const ETSI103097_v1_1_15 = 2;
MsgProtocol const IEEE16092_v3 = 3;
```

El tipo de clave privada para el ACF puede representarse de la siguiente manera:

```
typedef uint8_t PrivKeyType;
PrivKeyType const PrivKeyEncoding_Invalid = 0; // inválida (nula)
PrivKeyType const PrivKeyEncoding_Plaintext = 1; // la clave privada está en el registro
PrivKeyType const PrivKeyEncoding_NXP_SMX = 2; // la clave privada está en el SMX del NXP
PrivKeyType const PrivKeyEncoding_NXP_SMX2 = 3; // la clave privada está en el SMX2 del NXP
PrivKeyType const PrivKeyEncoding_Craton = 4; // la clave privada está en Autotalks Craton
PrivKeyType const PrivKeyEncoding_REL_V2X = 5;// la clave privada está en el hardware Renesas V2X
```

El contenido de los índices de mariposa del ACF puede depender de la longitud del campo, que puede ser de 0, 1 o 3. Si la longitud es 0, no hay índices de mariposa.

```
butterflyIndices[1] = {
    uint8_t     j; }          // índice de una credencial simultáneamente válida

butterflyIndices[3] = {
    uint8_t   j;              // índice de una credencial simultáneamente válida
    uint8_t   i[2]; }  // valor que identifica la semana en la que es válida la credencial
```

El encabezado para un ACF puede contener uno o más campos de la siguiente manera:

```
typedef struct {
    uint8_t     acfId[4];                 // Identificador ACF ("acf")
    uint8_t     fileformatVersion;        // número de versión del formato de archivo (3)
    MsgProtocol messageProtocol;          // mensaje protocolo de registros
    PrivKeyType signingKeyType;           // tipo de clave de firma
    uint8_t     butterflyIndicesLen;      // n.º de bytes en la mariposa
                                          // índices en cada registro (0, 1 o 3)
    uint8_t     privateReconValLen;       // n.º de bytes en el valor de reconstrucción
privada en cada registro
    uint8_t     signingKeyInfoLen;        // n.º de bytes en la información de clave de firma
en cada registro
    PrivKeyType decryptionKeyType;  // tipo de clave de encriptación
    uint8_t     decryptionKeyInfoLen;  // n.º de bytes en la información de clave de
descripción en cada registro
    uint8_t     certificateLen[2];        // n.º de bytes en un certificado, big endian
    uint8_t     startTime[4];             // tiempo de inicio del primer registro, Time32, big endian
    uint8_t     startInterval[4];         // tiempo entre tiempos de inicio consecutivos
en segundos, big endian
    uint8_t     numSimultaneous;          // n.º de credenciales simultáneamente válidas
    uint8_t     numRecords[4];            // n.º de registros de credenciales en el archivo, big
endian
    uint8_t     catSigningKeyInfoLen; // n.º de bytes en la información de clave de
firma de oruga
    uint8_t     catSigningKeyInfo[catSigningKeyInfoLen];   // información de clave
de firma de oruga
    uint8_t     aesKeyLen;                // n.º de bytes en la clave de AES para
expansión de clave de firma
    uint8_t     aesKey[aesKeyLen];  // clave de AES para expansión de clave de firma

} AcfHeader;
```

El formato de registro en un ACF puede contener uno o más campos de la siguiente manera:

```
typedef struct {
  uint8_t butterflyIndices[butterflyIndicesLen];      // índice de mariposa
  uint8_t privateReconVal[privateReconValLen];        // valor de reconstrucción privado
  uint8_t signingKeyInfo[signingKeyInfoLen];          // información de clave de firma,
big endian
  uint8_t decryptionKeyInfo[decryptionKeyInfoLen];// información de clave de
desencriptación, big endian
  uint8_t certificate[certificateLen];                // certificado
} AcfRecord;
```

El formato de ACF puede contener campos de la siguiente manera:

```
typedef struct {
  AcfHeader header;          // encabezado
  AcfRecord records[numRecords]; // registros
} AcfFile;
```

El ACF puede contener una credencial anónima precargada para su uso con vehículos que operan en Estados Unidos. Las credenciales pueden generarse a partir de una clave de oruga. Puede haber hasta 20 credenciales válidas simultáneamente por semana. Las claves privadas pueden protegerse utilizando el NXP SMX2. Como resultado, el encabezado del ACF puede comprender los siguientes valores:

acfId = "acf'
fileFormatVersion = 3
messageProtocol = IEEE_16092_2013
signingKeyType = PrivKeyEncoding_NXP_SMX2 (se aplica a la clave de firma de oruga)
butterflyIndicesLen = 1 (puesto que el índice i está en el certificado implícito, por lo que sólo se requiere j)
privReconValLen = 32 (puesto que los certificados anónimos de EE.UU. están implícitos y utilizan ECDSA-NIST-P256)
signingKeyInfoLen = 0 (puesto que la clave de firma real no está en este ACF o en el SMX2)
decryptionKeyType = PrivKeyEncodingJnvalid (puesto que los certificados anónimos no tienen claves de encriptación)
decryptionKeyInfoLen = 0 (puesto que los certificados anónimos no tienen claves de encriptación)
certificateLen = n.º de bytes en el certificado anónimo en cada registro
startTime = Time32 que codifica el tiempo de inicio de los primeros 20 certificados
startInterval = 604800 (una semana, expresada en segundos) numSimultaneous = 20 (puesto que hay 20 certificados válidos simultáneamente)
numRecords = 20n, donde n es el número de semanas de credenciales en este ACF
catSigningKeyInfoLen = n.º de bytes para representar el índice en el SMX2 para la ranura que contiene la clave de firma de oruga
catSigningKeyInfo = el índice en el SMX2 para la ranura que contiene la clave de firma de oruga
aesKeyLen = 16 (paraAES-128)
aesKey[16] = la clave AES para expandir la clave de firma de oruga

Cada uno de los 20n registros puede contener:

butterflyIndices[1] = el índice j que identifica la credencial en el conjunto de credenciales válidas simultáneamente,
privateReconVal[32] = el valor privado de reconstrucción para esta credencial,
certificate[certificateLen] = el certificado anónimo implícito para esta credencial.

El ACF puede contener una credencial anónima precargada para su uso con vehículos que operan en la Unión Europea. Las credenciales pueden generarse a partir de una clave de oruga. Puede haber hasta 20 credenciales válidas simultáneamente por semana. Las claves privadas pueden protegerse utilizando el NXP SMX2. Como resultado, el encabezado del ACF puede comprender los siguientes valores:

acfId = "acf'

fileFormatVersion = 3
messageProtocol = ETSI_103097_v1_1_15
signingKeyType = PrivKeyEncoding_NXP_SMX2 (se aplica a la clave de firma de oruga)
butterflyIndicesLen = 3 (puesto que estas no se encuentran en el certificado explícito anónimo)
privReconValLen = 0 (puesto que los certificados anónimos de la UE son explícitos)
signingKeyInfoLen = 0 (puesto que la clave de firma real no está en este ACF o en el SMX2)
decryptionKeyType = PrivKeyEncodingJnvalid (puesto que los certificados anónimos no tienen claves de encriptación)
decryptionKeyInfoLen = 0 (puesto que los certificados anónimos no tienen claves de encriptación)
certificateLen = n.º de bytes en el certificado anónimo en cada registro
startTime = Time32 que codifica el tiempo de inicio de los 20 certificados
startInterval = 604800 (una semana, expresada en segundos)
numSimultaneous = 20 (puesto que hay 20 certificados válidos simultáneamente)
numRecords = 20n, donde n es el número de semanas de credenciales en este ACF
catSigningKeyInfoLen = n.º de bytes para representar el índice en el SMX2 para la ranura que contiene la clave de firma de oruga
catSigningKeyInfo = el índice en el SMX2 para la ranura que contiene la clave de firma de oruga
aesKeyLen = 16 (paraAES-128)
aesKey[16] = la clave AES para expandir la clave de firma de oruga

Cada uno de los 20n registros puede contener:

butterfly Indices [3] = el índice j que identifica la credencial en el conjunto de credenciales válidas simultáneamente seguido del índice i que identifica la semana en la credencial es válida, y
certificate[certificateLen] = el certificado anónimo explícito para esta credencial.

Las credenciales pueden cambiarse una vez que caducan. Como se ha mencionado anteriormente, las credenciales pueden ser válidas durante un periodo, tal como una semana a la vez. Una vez que las credenciales caducan, deben obtenerse nuevas credenciales para su uso.

Una optimización proporcionada por las realizaciones ejemplares es para indizar los archivos de credenciales de modo que las credenciales no necesiten ser indexadas cada vez que se inicializa el sistema. Ciertos fabricantes de vehículos pueden desear precargar el vehículo con todas las credenciales necesarias para la vida útil prevista del vehículo o una parte significativa de la vida útil del vehículo. Debido a que esto constituye un gran número de credenciales, podría llevar mucho tiempo localizar y obtener todas las credenciales para una venta de tiempo dada. Las realizaciones ejemplares proporcionan un enfoque para acceder de un modo eficiente a los archivos de credenciales de una manera que consume sustancialmente menos tiempo.

La FIG. 7 es un diagrama de flujo 700 de las etapas que se realizan para indizar los archivos de credenciales para un LCM dado. Inicialmente, las credenciales se almacenan en un archivo de credenciales nombrado (etapa 702). Como se ha explicado anteriormente, los nombres de los archivos de credenciales pueden incluir la fecha en la cual el archivo de credenciales está activo o expira, por ejemplo. Se proporciona un índice a los archivos de credenciales de modo que puedan localizarse fácilmente todos los archivos de credenciales para una duración dada. En particular, las credenciales se almacenan según el momento de inicio en el cual son válidas y se crea un índice cronológico para los archivos de credenciales y se almacena en el vehículo (etapa 704). Cuando se necesitan nuevas credenciales, el índice se utiliza para recuperar la credencial durante una duración dada (etapa 706). Se recupera al menos uno de los archivos de credenciales.

Las realizaciones ejemplares también pueden proporcionar otra optimización prederivando claves de modo que no existe la necesidad de derivar las claves bajo demanda. La derivación de claves puede llevar tiempo, y por lo tanto puede dar como resultado una latencia significativa cuando se derivan las claves bajo demanda.

Según se muestra en la Fig. 8, cuando se inicia un administrador local de certificados para el sistema de comunicación segura para vehículos (etapa 802), se hace una comprobación de si hay suficientes claves privadas (etapa 806). Si no las hay, deben derivarse más claves privadas (etapa 808). Las claves se derivan preferiblemente en un hardware segundo (por ejemplo un HSM) de modo que se elimina la posibilidad de que un intruso obtenga acceso a las claves o a otra información segura. Los expertos en la técnica apreciarán que puede haber una diversidad de algoritmos y enfoques diferentes para derivar las claves. Las claves privadas pueden derivarse, por ejemplo, utilizando claves de mariposa. Si hay suficientes claves privadas, las claves prederivadas se almacenan en un almacén no volátil para su uso por el sistema de comunicación segura para vehículos (etapa 810). Estas claves privadas que se han usado en una comunicación según se ha necesitado (etapa 812).

Para mejorar la privacidad del sistema de comunicación segura para vehículos, es deseable cambiar la identidad de la parte de forma continua. La FIG. 9 proporciona un diagrama de flujo 900 de las etapas que pueden formarse para realizar el cambio de identidad. Inicialmente, se recibe una petición para cambiar la identidad (etapa 902). Esta petición puede ser a instancias de una parte o puede ser impuesta por el sistema en momentos específicos o en ciertos eventos. Entonces, el sistema de comunicaciones del vehículo identifica qué certificados digitales están disponibles

para su selección para realizar la nueva identidad de la parte (etapa 904). Se recibe una selección (etapa 906) y se devuelve el certificado seleccionado o se devuelve un identificador al certificado seleccionado (etapa 908). Después, este certificado seleccionado se utiliza en lugar del certificado anterior. Este cambio de certificados actúa como un punto de sincronización y puede sincronizarse cambiando otros identificadores de identidad (tales como una dirección MAC) de modo que esos identificadores también pueden actualizarse al mismo tiempo (etapa 912).

Es deseable proporcionar una capa de abstracción para uso interno con las bibliotecas que proporcionan la funcionalidad criptográfica. Las realizaciones ejemplares proporcionan una interfaz de programa de aplicación (API) que sirve como una capa de abstracción de hardware. El hardware de seguridad puede ser de diferentes proveedores con diferentes interfaces. Esta API permite que las funciones y las firmas de llamadas a funciones sean uniformes para su uso interno. El código para realizar las funciones específicas puede adaptarse al dispositivo de hardware de seguridad implicado. Como se describirá con mayor detalle más adelante, puede proporcionarse el hardware seguro, por ejemplo, para proteger claves privadas y/o para acelerar la verificación.

La FIG. 10 representa un diagrama de flujo 1000 del uso de dicha API en realizaciones ejemplares. Se proporciona una API para los métodos criptográficos proporcionados en una biblioteca de métodos de seguridad (etapa 1002). Se recibe una llamada a un método y se realiza a través de la API (etapa 1004). El método adecuado está implicado en la (etapa 1006). El método puede ser cualquiera de una diversidad de métodos diferentes detallados más adelante, por ejemplo.

En realizaciones ejemplares, la API puede soportar una diversidad de tipos diferentes de objetos que tienen métodos asociados. Uno de esos objetos es un objeto de clave pública que tiene métodos y atributos asociados con una clave pública. El objeto puede contener la clave pública. Puede haber un método para encriptar usando la clave pública. Estos pueden ser un método para derivar una clave pública desde un certificado implícito. Puede haber un método para la verificación de firma.

También puede haber un objeto de clave privada para contener atributos y métodos asociados con una clave privada. El objeto puede contener una clave privada. Los métodos pueden incluir un método de desencriptado para desencriptar el texto cifrado y un método de firma para tomar datos y devolver una firma digital. Los métodos pueden incluir un método para crear una clave privada cuando se utilizan certificados implícitos y un método para derivar una clave privada basada en claves de mariposa.

También puede haber un objeto de clave simétrica que produce textos cifrados de texto plano. Usando el estándar de encriptación avanzada (AES), que es un algoritmo de encriptación simétrica. Puede haber un método de desencriptado correspondiente para desencriptar texto cifrado para producir texto plano.

Puede proporcionarse un objeto hash para un algoritmo hash asociado. Pueden proporcionarse métodos para recibir el contenido que va a convertirse en hash y producir una función hash de los contenidos.

La FIG. 11 muestra un ejemplo de la organización del sistema de comunicación segura para vehículos en realizaciones ejemplares. El sistema representado en la FIG. 11 es para un solo vehículo o una sola unidad a pie de carretera. El vehículo o una unidad a pie de carretera incluye una unidad de abordo 1100 que es responsable para comunicarse inalámbricamente con otros vehículos, unidades a pie de carretera y similares. Además, la unidad de abordo 1100 es responsable de realizar otras funcionalidades, tales como proporcionar servicios a aplicaciones. La unidad de abordo 1100 puede interactuar con una diversidad de unidades de aplicación 1102, 1104 y 1106. Cada unidad de aplicación es responsable de ejecutar una o más aplicaciones 1103, 1105 y 1107, respectivamente. Las aplicaciones 1103, 1105 y 1107 pueden ejecutarse en un procesador común y el procesador puede ser parte de la unidad de abordo 1100.

La FIG. 12 ilustra en mayor detalle algunos de los componentes encontrados en la unidad de abordo 1100, así como algunos dispositivos periféricos que pueden comunicarse con la unidad de abordo 1100 cuando está presente en un vehículo. Como se muestra en la FIG. 12, la lógica de procesamiento 1200 puede proporcionarse para proporcionar capacidad de procesamiento para la unidad de abordo. La lógica de procesamiento 1200 puede tener acceso al almacén 1204. La lógica de procesamiento 1200 puede ser similar para una unidad a pie de carretera. El almacén puede tomar una diversidad de formatos diferentes, incluyendo un almacén no volátil, un almacén de estado sólido, un almacén en un medio legible por ordenador y similares. La lógica de procesamiento 1200 puede acoplarse a una interfaz de red inalámbrica 1202. La interfaz de red inalámbrica 1202 puede proporcionar la capacidad de comunicarse con una red inalámbrica, tal como una red 802.11P. La lógica de procesamiento también puede interactuar con una diversidad de dispositivos periféricos, incluyendo un transceptor 1206 de un sistema de posicionamiento global (GPS), una pantalla de vídeo 1208, una cámara 2010 y sensores 1212.

La lógica de procesamiento puede tomar muchas formas diferentes. Por ejemplo, la lógica de procesamiento 1300 puede incluir una matriz de puertas programable en campo (FPGA) 1302, un circuito integrado específico de la aplicación (ASIC) 1304 y/o un microprocesador 1306. La lógica de procesamiento puede encontrarse, por ejemplo, en un sistema integrado que realiza la funcionalidad de la unidad de abordo.

La FIG. 14 representa la interacción entre la aplicación 1400 y las funcionalidades protegidas que se proporcionan como parte de la seguridad para el sistema de comunicación segura para vehículos. Las funcionalidades protegidas 1402 incluyen servicios criptográficos 1404 y almacenamiento y gestión de claves 1406. Los servicios criptográficos realizan métodos criptográficos, tales como encriptación, desencriptación, firmas digitales y similares. El almacenamiento y gestión de claves 1406 se proporciona para almacenar claves que se usan para los servicios criptográficos y para gestionar dichas claves. Se proporciona una interfaz protegida 1416 para el servicio criptográfico y se proporciona otra interfaz protegida 1418 para la gestión del almacén de claves. Pueden almacenarse, por ejemplo, en un hardware seguro. El hardware seguro puede usarse para almacenar las claves privadas y para realizar operaciones de clave privada. El hardware seguro puede incluir hardware tanto de almacén como de procesamiento. El hardware seguro puede asegurarse físicamente y puede estar diseñado para evitar el monitoreo y la manipulación.

Cuando una de las aplicaciones 1400 desea servicios criptográficos, la aplicación envía una petición para servicios criptográficos 1410 a los servicios criptográficos 1404 a través de la interfaz protegida 1416. Si los servicios criptográficos necesitan una clave, la clave se obtiene desde el almacenamiento y gestión de claves 1406. Los servicios criptográficos utilizan la clave que necesitan y devuelven el resultado 1412 a la aplicación 1400 a través de la interfaz protegida 1416. En algunos casos, las solicitudes pueden estar encriptadas y requieren una clave que se envía desde la aplicación 1400 a través de la interfaz protegida 1418 al almacenamiento y gestión de claves 1406.

Aunque la presente invención se ha descrito con referencia a realizaciones ejemplares en el presente documento, los expertos en la técnica apreciarán que pueden realizarse diversos cambios en la formar y los detalles sin alejarse del alcance pretendido de la presente invención según se define mediante las reivindicaciones que siguen.

REIVINDICACIONES

1. Un método para su uso en un sistema de comunicación segura para vehículos, comprendiendo el método:
almacenar (702) credenciales durante una vida útil prevista de un vehículo o una parte significativa de la vida útil prevista de un vehículo en archivos de credenciales en un almacén en el vehículo, en el que cada credencial incluye una clave privada de firma y un certificado digital y es válida durante un marco de tiempo específico;

nombrar (702) los archivos de credenciales para que tengan nombres que contengan información con respecto a los marcos de tiempo específicos de las credenciales en los archivos de credenciales;
almacenar (704) un índice de los archivos de credenciales en el almacén del vehículo usando los nombres, en el que el índice indexa los archivos de credenciales por los marcos de tiempo específicos en los que las credenciales almacenadas en los archivos de credenciales son válidas;
usar (706) el índice para recuperar los archivos de credenciales durante un periodo, en el que las credenciales en los archivos de credenciales recuperados son válidas durante el periodo; y
usar al menos uno de los archivos de credenciales recibidos en el sistema de comunicación segura para vehículos durante el periodo.

2. El método, según la reivindicación 1, que comprende además:
clasificar los archivos de credenciales por los marcos de tiempo específicos en los que son válidas las credenciales en los archivos de credenciales.

3. El método, según la reivindicación 2, en el que la clasificación utiliza los nombres de los archivos de credenciales para clasificar.

4. El método, según la reivindicación 3, que comprende además: crear el índice para indexar los archivos de credenciales clasificados.

5. Un medio de almacenamiento no transitorio legible por ordenador que contiene instrucciones que, cuando se ejecutan por la lógica de procesamiento, realizan lo siguiente:

almacenar (702) credenciales durante una vida útil prevista de un vehículo o una parte significativa de la vida útil prevista de un vehículo en archivos de credenciales en un almacén en el vehículo, en el que cada credencial incluye una clave privada de firma y un certificado digital y es válida durante un marco de tiempo específico;
nombrar (702) los archivos de credenciales para que tengan nombres que contengan información con respecto a los marcos de tiempo específicos de las credenciales en los archivos de credenciales;
almacenar (704) un índice de los archivos de credenciales en el almacén del vehículo usando los nombres, en el que el índice indexa los archivos de credenciales por los marcos de tiempo específicos en los que las credenciales almacenadas en los archivos de credenciales son válidas;
usar (706) el índice para recuperar los archivos de credenciales durante un periodo, en el que las credenciales en los archivos de credenciales recuperados son válidas durante el periodo; y
usar al menos uno de los archivos de credenciales recibidos en el sistema de comunicación segura para vehículos durante el periodo.

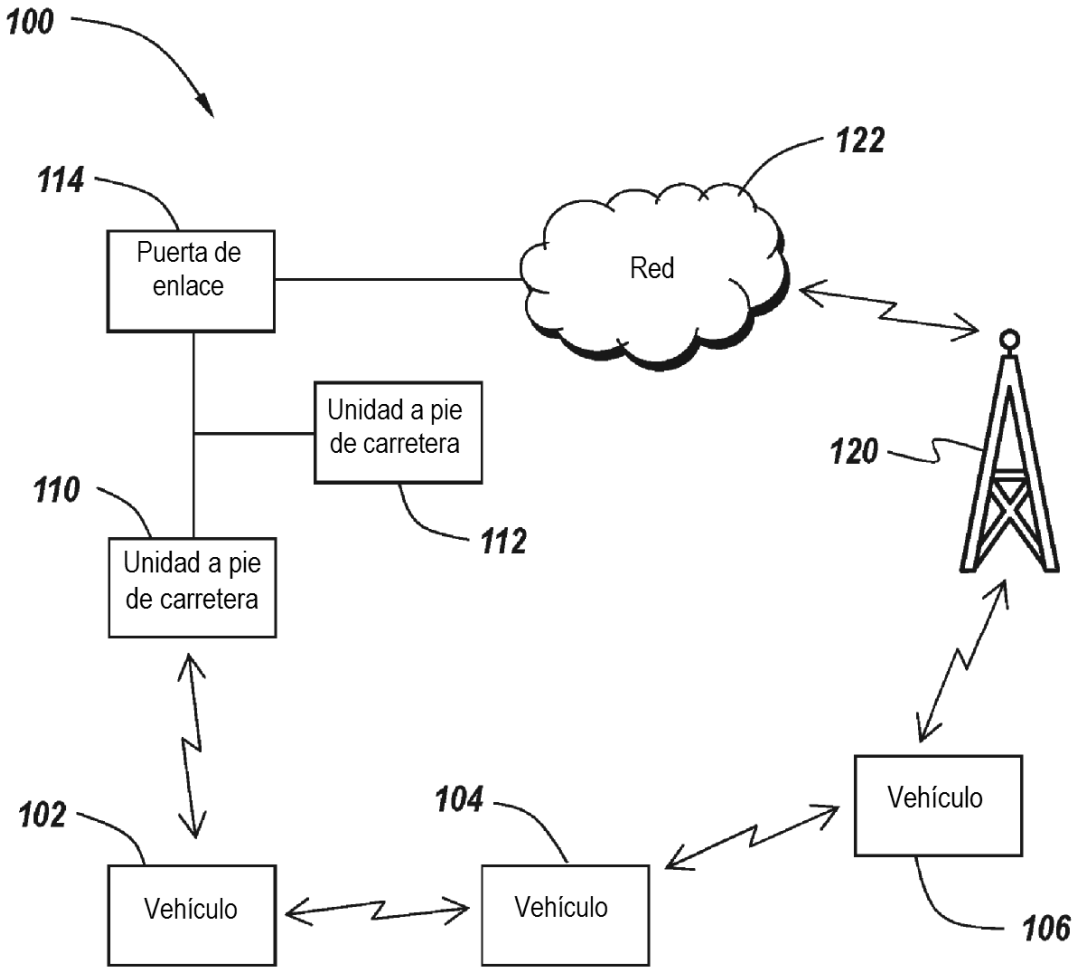
100
114
Puerta de enlace
122
Red
Unidad a pie de carretera
112
110
Unidad a pie de carretera
120
102
Vehículo
104
Vehículo
Vehículo
106

Fig. 1

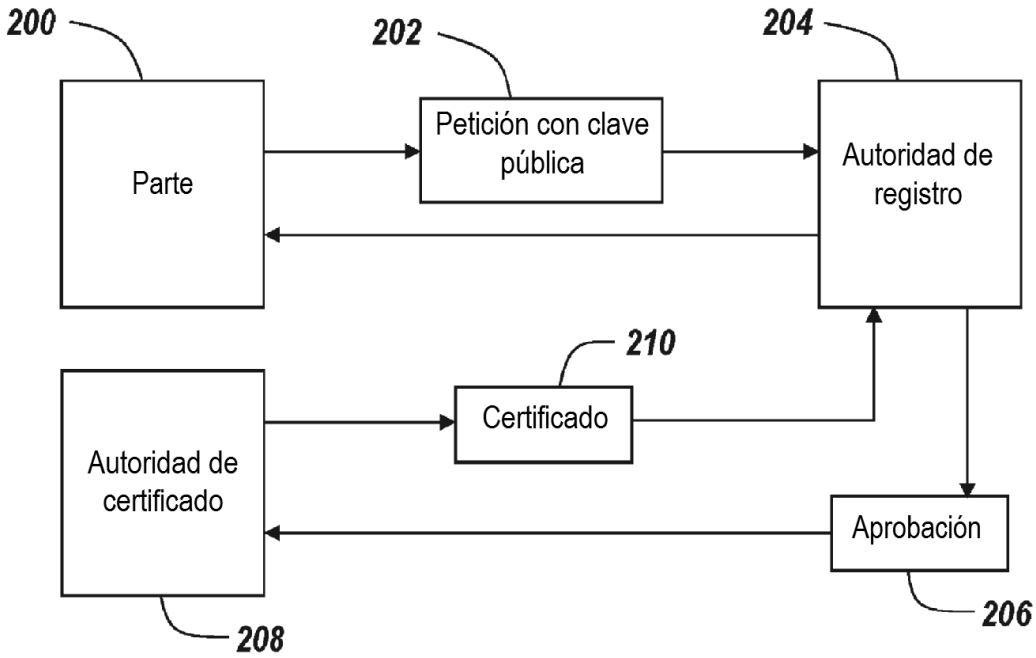
200
202
204
Parte
Petición con clave pública
Autoridad de registro
210
Certificado
Autoridad de certificado
Aprobación
206
208

Fig. 2

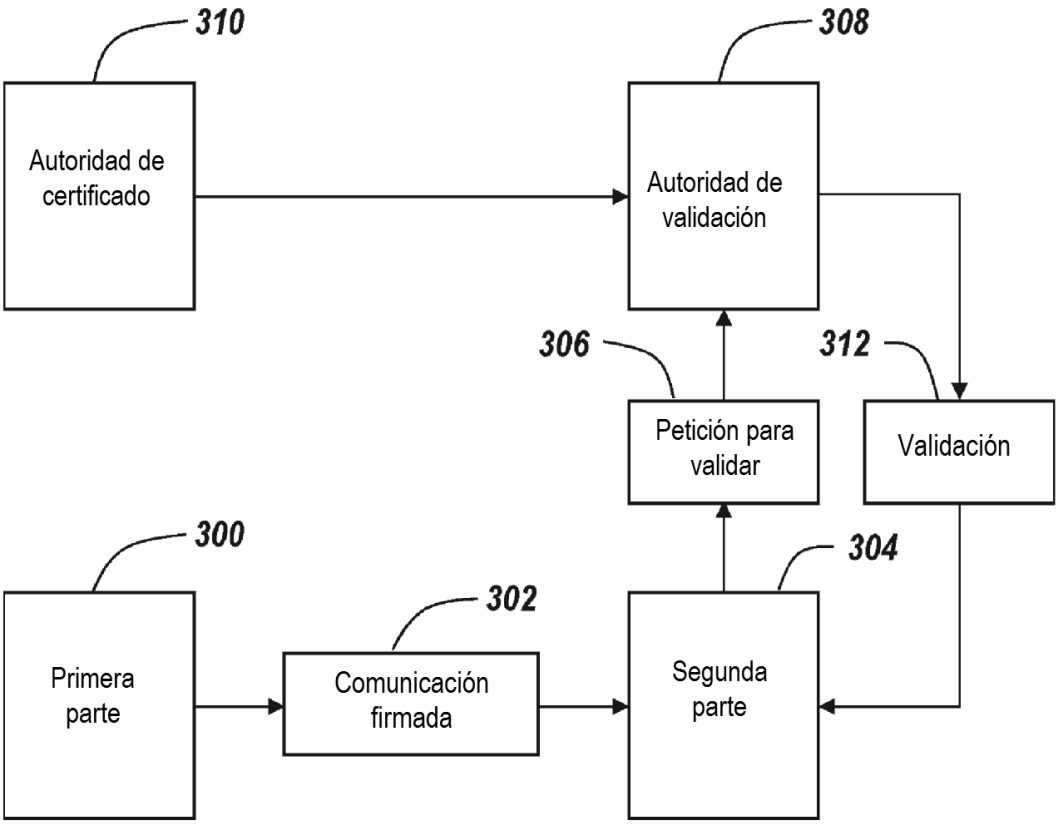
310
Autoridad de certificado
308
Autoridad de validación
306
Petición para validar
312
Validación
300
Primera parte
302
Comunicación firmada
304
Segunda parte

Fig. 3

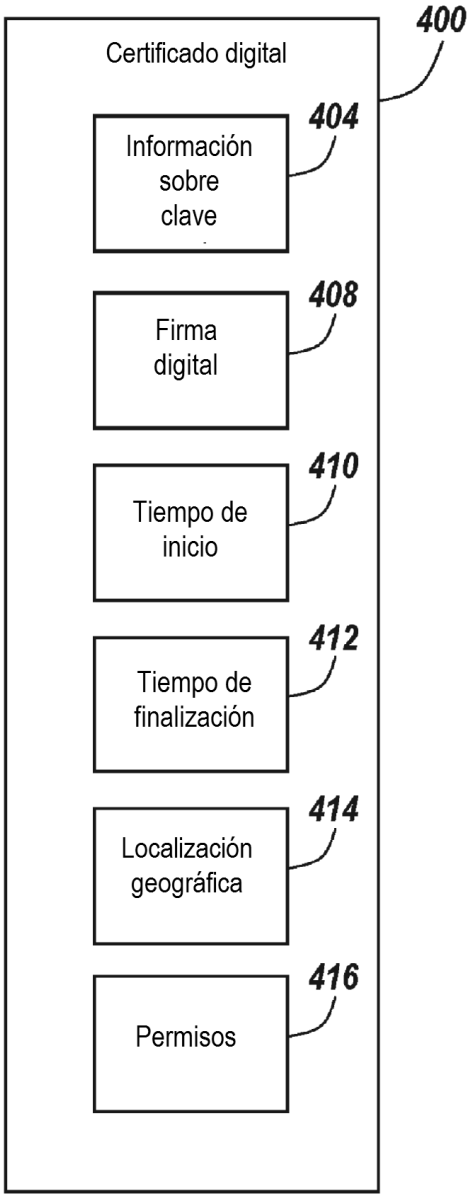
400
Certificado digital
404
Información sobre clave
408
Firma digital
410
Tiempo de inicio
412
Tiempo de finalización
414
Localización geográfica
416
Permisos

Fig. 4

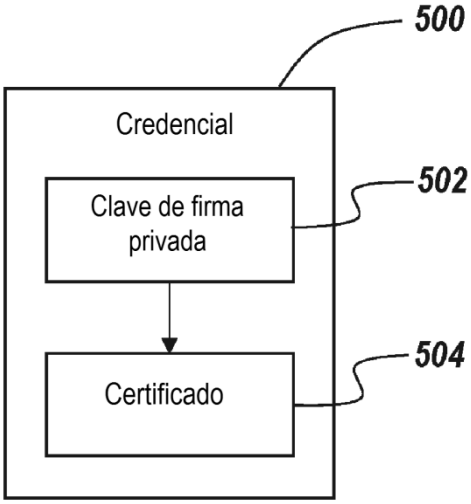

Fig. 5

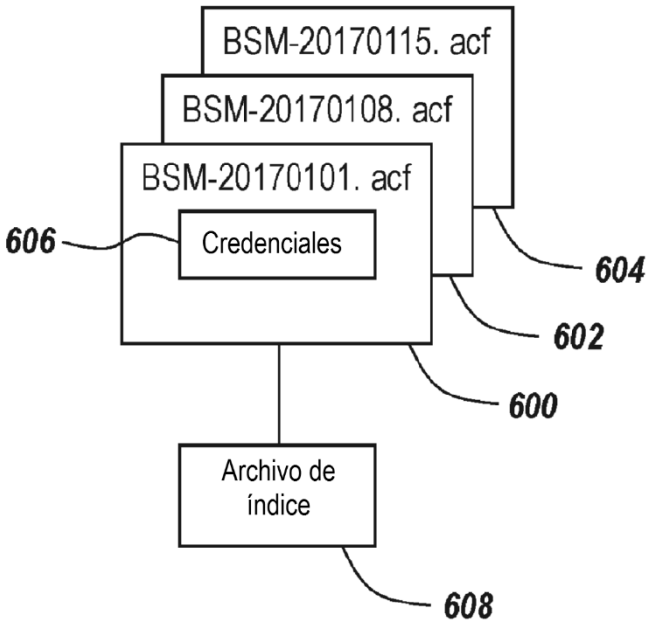
BSM-20170115. acf
BSM-20170108. acf
BSM-20170101. acf
Credenciales
606
604
602
600
Archivo de índice
608

Fig. 6

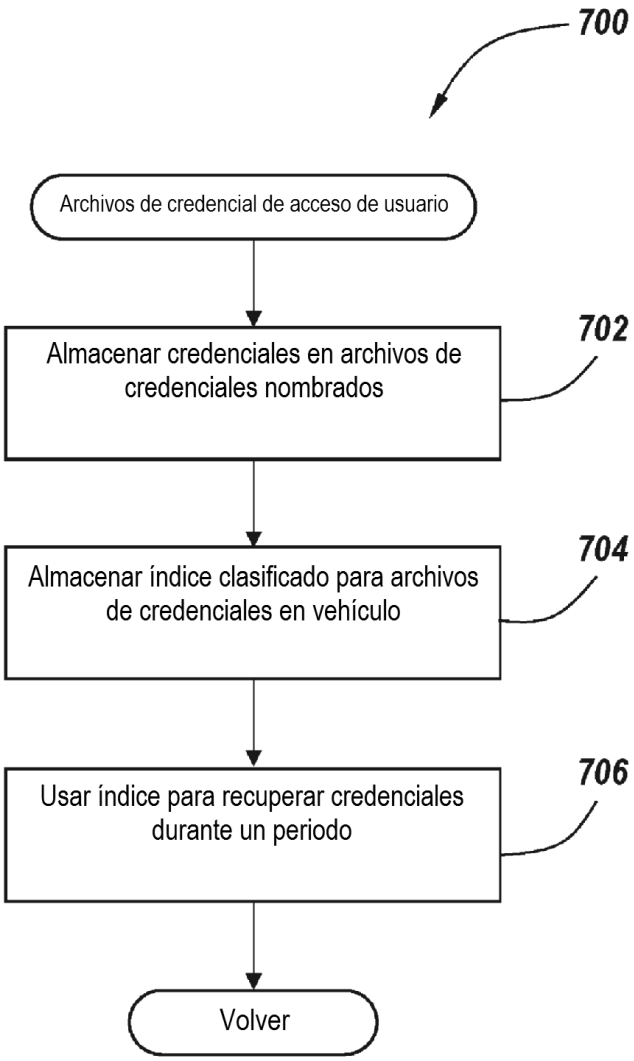
700
Archivos de credencial de acceso de usuario
Almacenar credenciales en archivos de credenciales nombrados
702
Almacenar índice clasificado para archivos de credenciales en vehículo
704
Usar índice para recuperar credenciales durante un periodo
706
Volver

Fig. 7

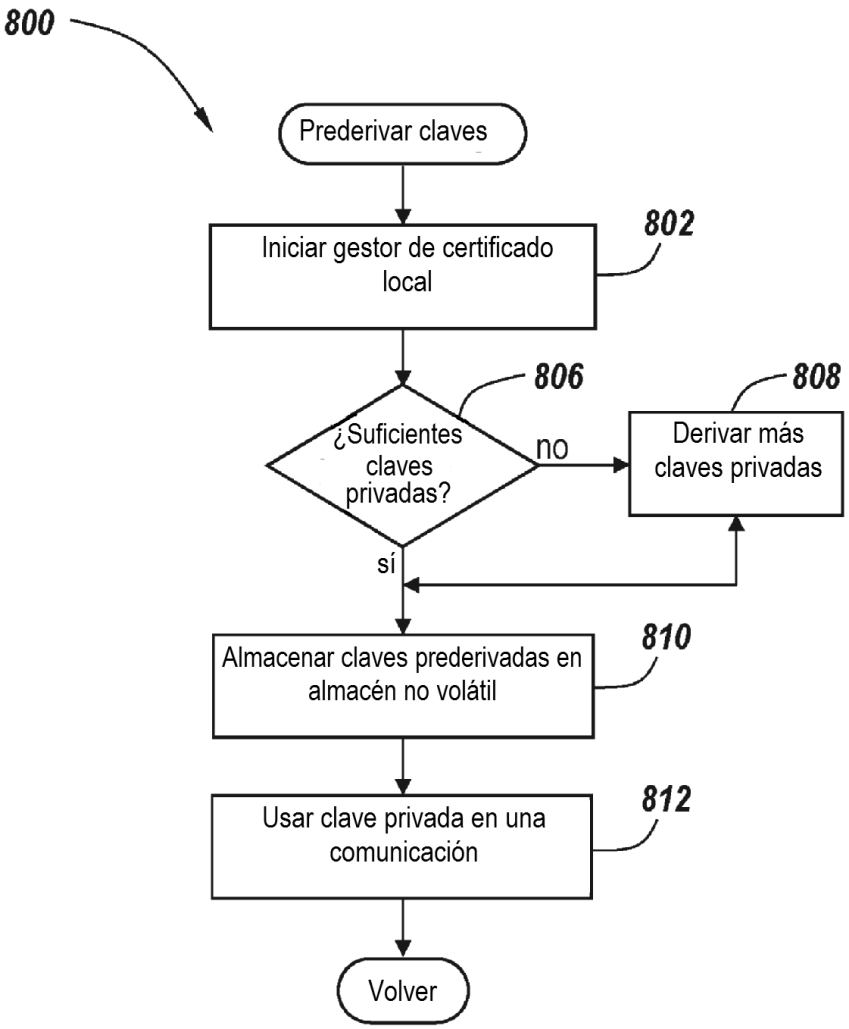
800
Prederivar claves
Iniciar gestor de certificado local
802
806
¿Suficientes claves privadas?
no
808
Derivar más claves privadas
sí
Almacenar claves prederivadas en almacén no volátil
810
Usar clave privada en una comunicación
812
Volver

Fig. 8

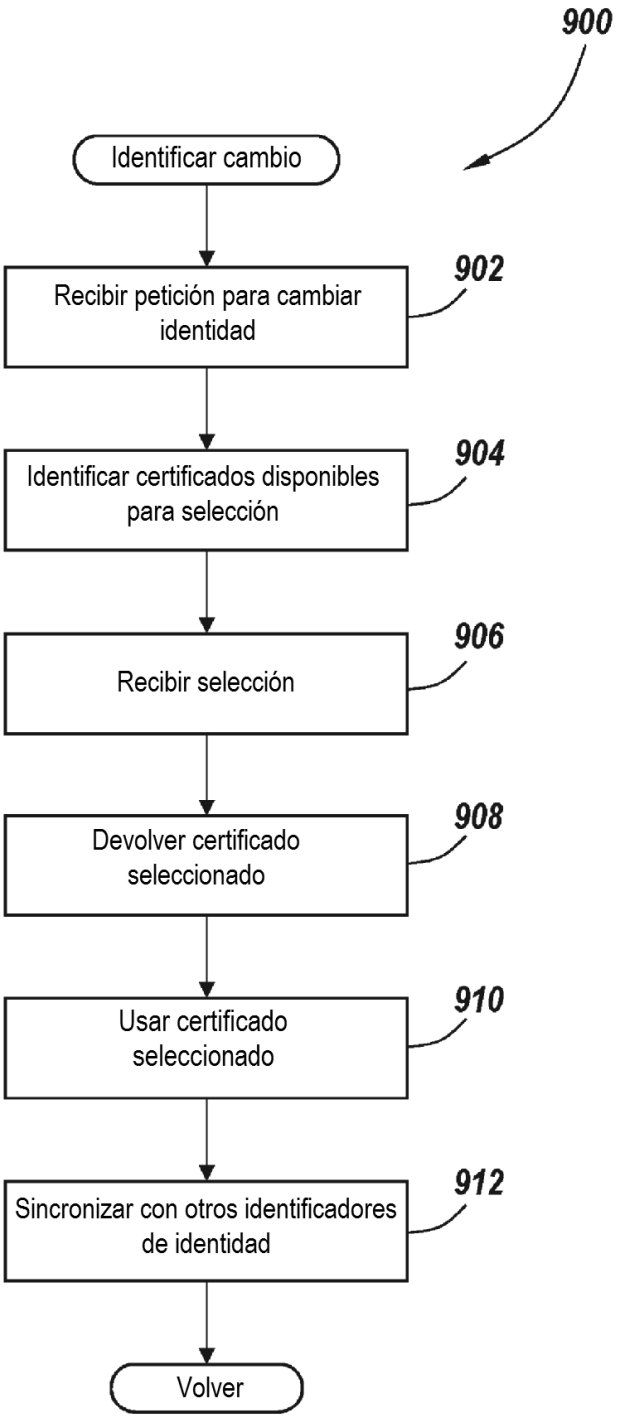
900
Identificar cambio
902
Recibir petición para cambiar identidad
904
Identificar certificados disponibles para selección
906
Recibir selección
908
Devolver certificado seleccionado
910
Usar certificado seleccionado
912
Sincronizar con otros identificadores de identidad
Volver

Fig. 9

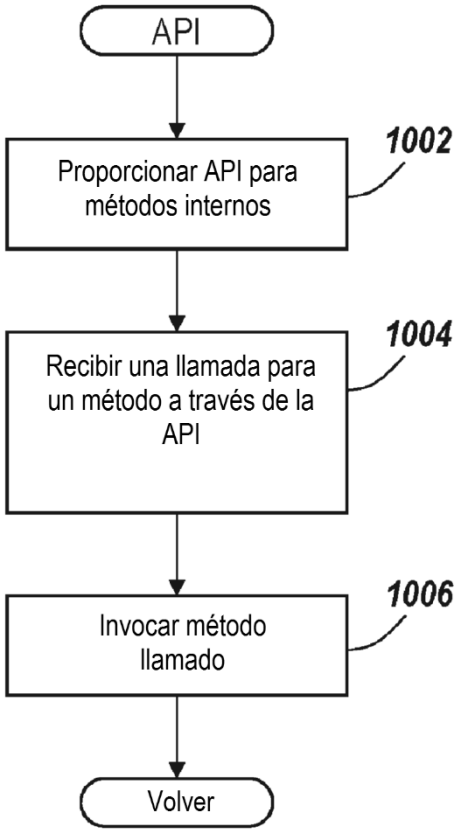
API
Proporcionar API para métodos internos
1002
Recibir una llamada para un método a través de la API
1004
Invocar método llamado
1006
Volver

Fig. 10

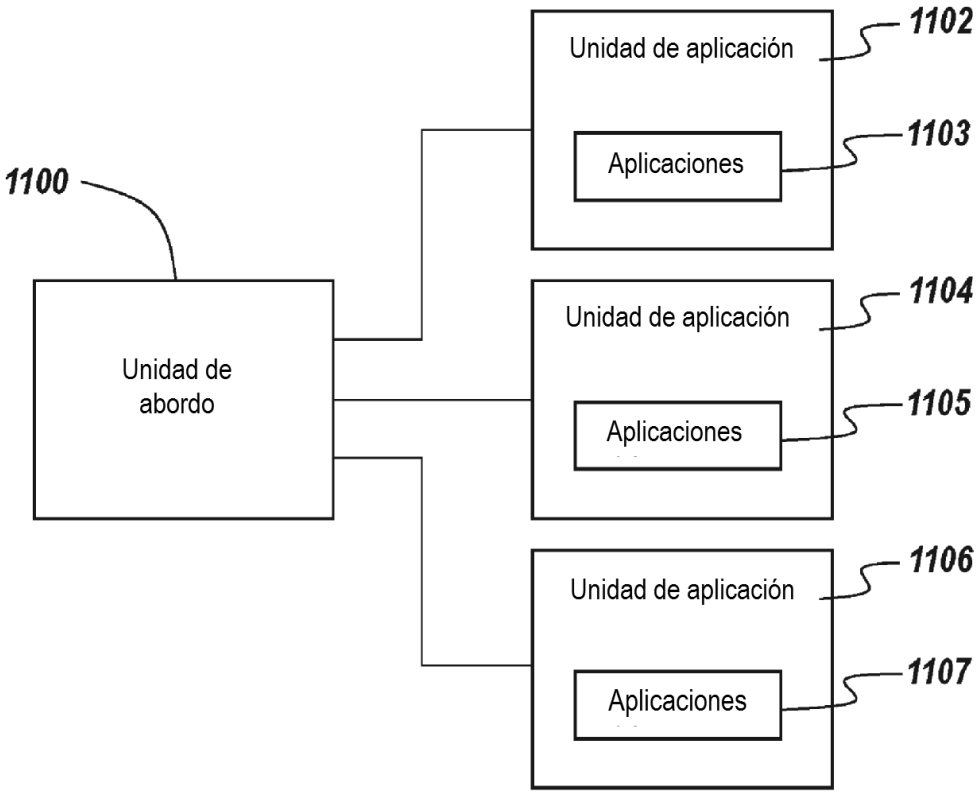
1100
Unidad de abordo
Unidad de aplicación
1102
Aplicaciones
1103
Unidad de aplicación
1104
Aplicaciones
1105
Unidad de aplicación
1106
Aplicaciones
1107

Fig. 11

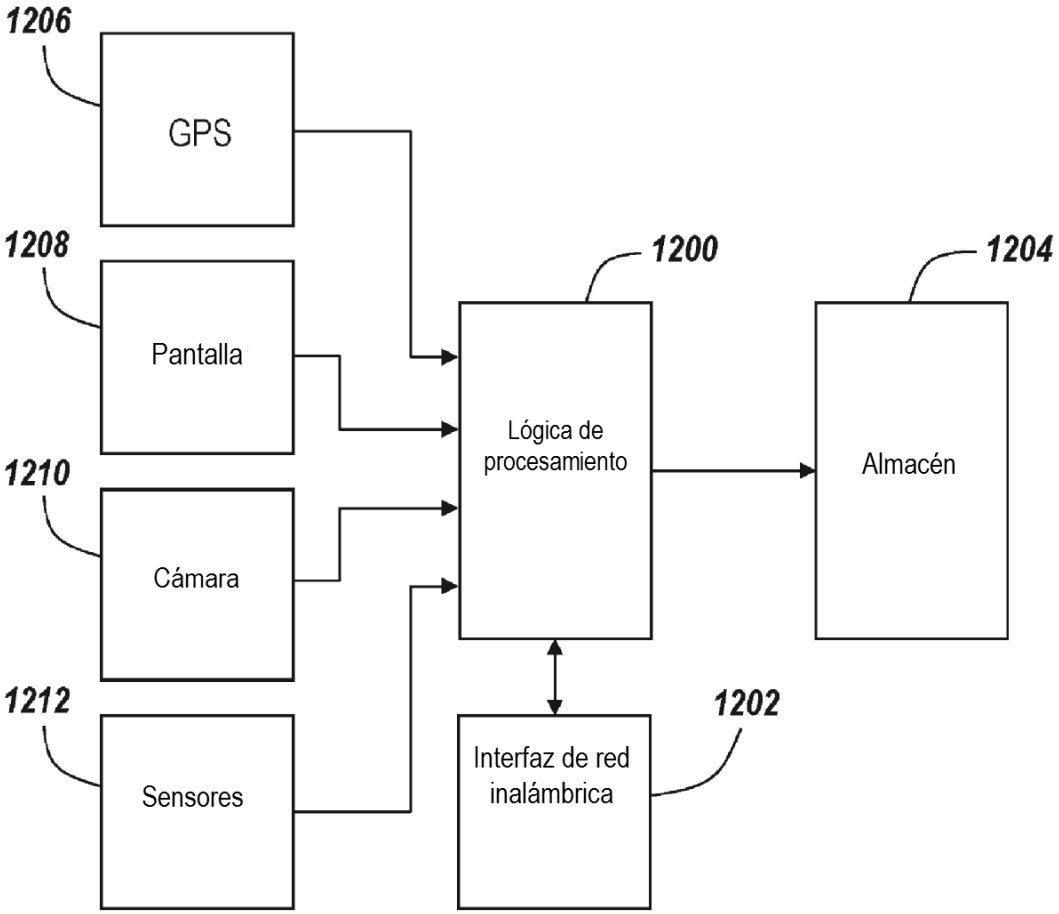
1206
GPS
1208
Pantalla
1210
Cámara
1212
Sensores
1200
Lógica de procesamiento
1204
Almacén
1202
Interfaz de red inalámbrica

Fig. 12

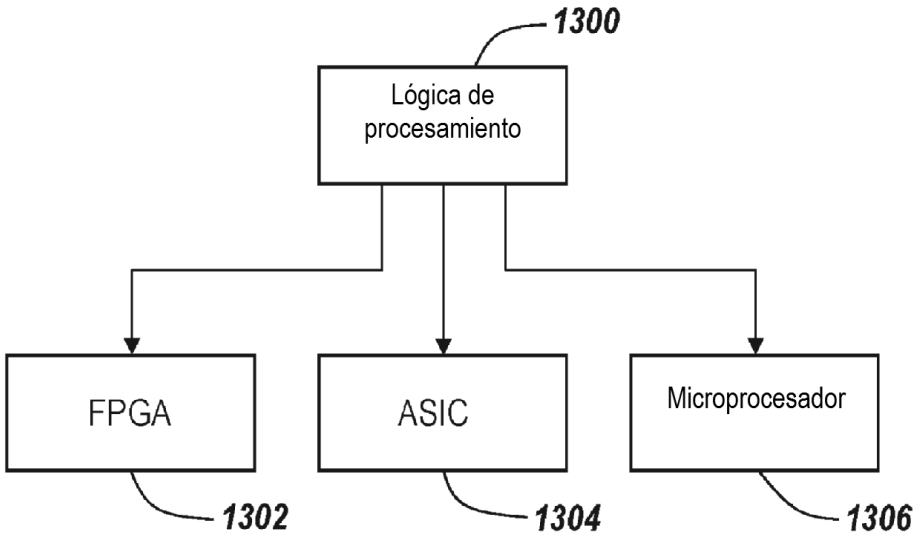
1300
Lógica de procesamiento
FPGA
ASIC
Microprocesador
1302
1304
1306

Fig. 13

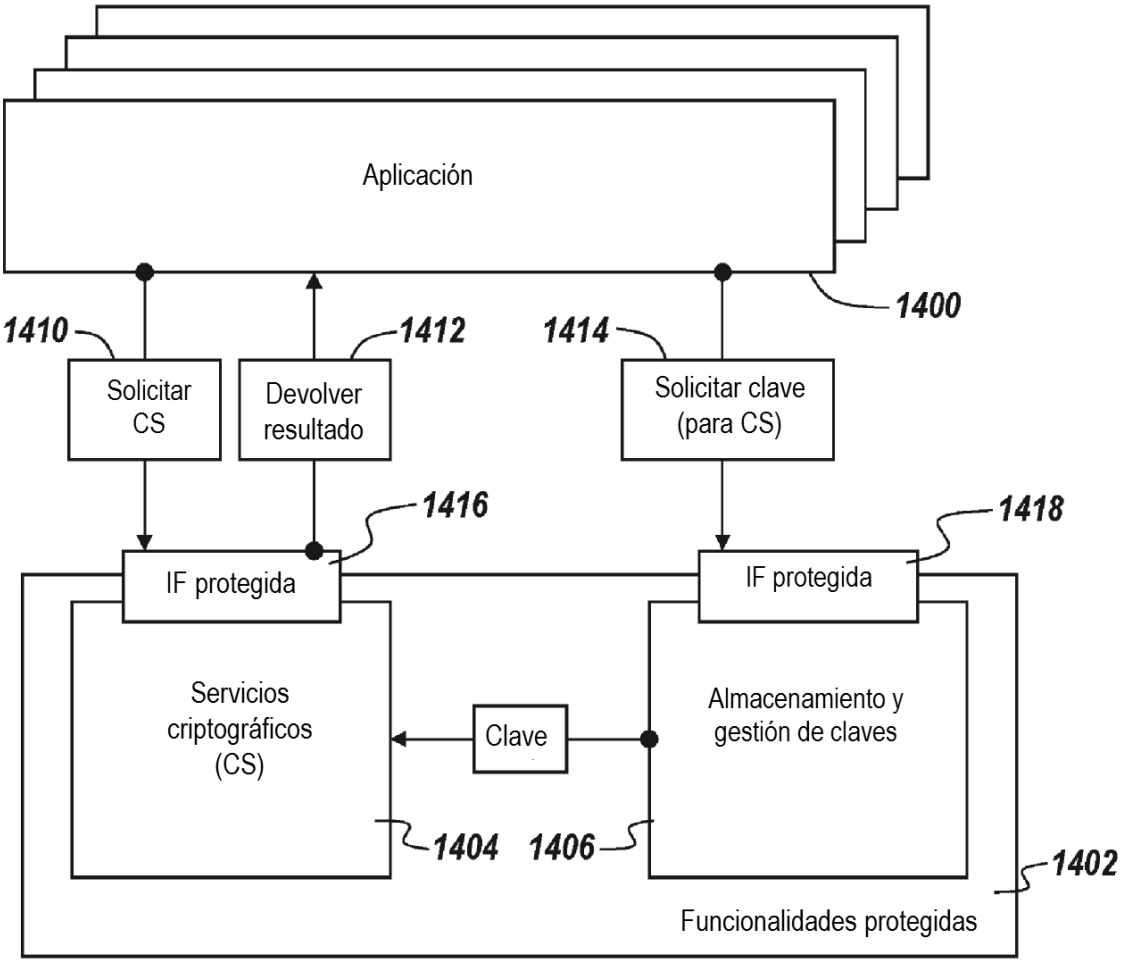
Aplicación
1400
1410
1412
1414
Solicitar CS
Devolver resultado
Solicitar clave (para CS)
1416
1418
IF protegida
IF protegida
Servicios criptográficos (CS)
Clave
Almacenamiento y gestión de claves
1404
1406
1402
Funcionalidades protegidas

Fig. 14