Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1372

(03/2020)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios seguros (2) – Seguridad de los sistemas de transporte inteligentes (STI)

Directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X)

Recomendación UIT-T X.1372

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	**X.1370–X.1379**
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1372

Directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X)

Resumen

En la Recomendación UIT-T X.1372 se presentan directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X). El término genérico V2X designa los modos de comunicación conocidos como vehículo a vehículo (V2V), vehículo a infraestructura (V2I), vehículo a dispositivos nómadas (V2D) y vehículo a peatón (V2P), que se abordan en esta Recomendación.

En los últimos años se ha experimentado una evolución consecuente de las Comunicaciones vehiculares en el entorno de los sistemas de transporte inteligentes (STI). La comunicación V2X mejora notablemente la seguridad vial, reduce la congestión del tráfico y aumenta la comodidad. Sin embargo, la comunicación V2X hace que entidades importantes del entorno STI sean vulnerables a ciberataques de distintos tipos.

Para resolver ese problema de seguridad, en esta Recomendación se identifican las amenazas presentes en el entorno de comunicación V2X y se especifican los requisitos de seguridad de la comunicación V2X para contrarrestar esas amenazas. En esta Recomendación se describen también la posible implementación segura de la comunicación V2X.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1372	2020-03-26	17	11.1002/1000/14091

Palabras clave

Análisis de amenazas, análisis de riesgos, requisitos de seguridad, seguridad STI, V2D, V2I, V2P, V2V, V2X.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T X.1372

Directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X)

1 Alcance

En esta Recomendación se presentan directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X). V2X ("entre el vehículo y su entorno") es un término genérico para los modos de comunicación conocidos como vehículo a vehículo (V2V), vehículo a infraestructura (V2I), vehículo a dispositivos nómadas (V2D) y vehículo a peatón (V2P), que se abordan en esta Recomendación. En esta Recomendación se identifican las amenazas presentes en el entorno de comunicación V2X y se especifican los requisitos de seguridad de la comunicación V2X para contrarrestar esas amenazas. Se describe también la posible implementación segura de la comunicación V2X.

Quedan fuera del alcance de esta Recomendación los controles de seguridad específicos para la comunicación V2X.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza los términos siguientes definidos en otros documentos:

3.1.1 imputabilidad [b-UIT-T X.800]: propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad.

3.1.2 autenticidad [b-UIT-T X.641]: protección para la autentificación mutua y la autentificación del origen de los datos.

3.1.3 autentificación [b-UIT-T X.1252]: proceso encaminado a lograr una confianza suficiente en la vinculación entre la entidad y la identidad presentada.

NOTA – En el contexto de la gestión de identidad (IdM) se entiende que el término autentificación se refiere a la autentificación de una entidad.

3.1.4 autorización [b-UIT-T X.800]: atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.1.5 disponibilidad [b-UIT-T X.800]: propiedad de ser accesible y utilizable a petición por una entidad autorizada.

3.1.6 autoridad de certificación [b-UIT-T X.509]: autoridad a la cual uno o más usuarios han confiado la creación y firma digital de certificados de clave pública. Facultativamente, la autoridad de certificación puede crear las claves de los usuarios.

3.1.7 confidencialidad [b-UIT-T X.800]: propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.8 integridad [b-UIT-T X.800]: propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.1.9 código de mensaje de autentificación (MAC, *message authentication code*) [b-UIT-T X.813]: valor de verificación criptográfica utilizado para garantizar la autentificación del origen de los datos y la integridad de los datos.

3.1.10 dispositivo nómada [b-UIT-T F.749.1]: se denomina dispositivo nómada a todo dispositivo de información y comunicación, así como de ocio, que pueden introducir el conductor y/o los pasajeros en el vehículo para utilizarlos cuando éste está en marcha. Son, por ejemplo, los teléfonos móviles, los ordenadores portátiles, las tabletas, los dispositivos de navegación móvil, los reproductores de medios portátiles y los teléfonos inteligentes multifuncionales.

3.1.11 no repudio con prueba del origen [b-UIT-T X.800]: se proporciona al destinatario de los datos la prueba del origen de los datos. Esto lo protegerá contra cualquier tentativa del expedidor de negar que ha enviado los datos o su contenido.

3.1.12 seudónimo [b-UIT-T X.1252]: un identificador cuya vinculación con una entidad no se conoce o sólo se conoce hasta cierto grado dentro del contexto en el cual se utiliza.

NOTA – Los seudónimos pueden utilizarse para evitar o reducir los riesgos relativos a la privacidad que entraña la utilización de relaciones de identificador que pueden revelar la identidad de la entidad.

3.1.13 certificado de clave pública (PKC, *public-key certificate*) [b-UIT-T X.509]: clave pública de una entidad, junto con alguna otra información, hecha infalsificable por firma digital con la clave privada de la autoridad de certificación que la emitió.

3.2 Términos definidos en esta Recomendación

Esta Recomendación define los términos siguientes:

3.2.1 comportamiento indebido: comportamiento que resulta en el envío por los dispositivos de información errónea que puede hacer que otros dispositivos actúen de manera incorrecta. Denota también el comportamiento de los dispositivos que, habiendo recibido la información correcta, actúan de manera errónea.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

AES Norma de encriptación avanzada (*advanced encryption standard*)

AVN Audio, vídeo y navegación (*audio, video, and navigation*)

CA Autoridad de certificación (*certification authority*)

CAMP Crash Avoidance Metrics Partnership

CCM Código de autentificación de mensaje en modo contador con concatenación de bloques cifrados (*counter mode with cipher block chaining message authentication code*)

CCU Unidad central de comunicación (*central communication unit*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

EEBL Luces de freno de emergencia electrónicas (*electronic emergency brake light*)

ECDSA	Algoritmo de firma digital de curva elíptica (*elliptic curve digital signature algorithm*)
ECIES	Esquema de encriptación integrada de curva elíptica (*elliptic curve integrated encryption scheme*)
ECU	Unidad de control electronica (*electronic control unit*)
GPS	Sistema de posicionamiento global (*global positioning system*)
HDMI	Interfaz multimedios de alta definición (*high-definition multimedia interface*)
ID	Identificador (*identifier*)
IIP	Información de identificación personal
IVN	Red intravehicular (*in-vehicle network*)
KDF	Función de derivación de claves (*key derivation function*)
LDM	Mapa dinámico local (*local dynamic map*)
LOS	Línea de visibilidad directa (*line of sight*)
LTE	Evolución a largo plazo (*long term evolution*)
MAC	Código de autentificación de mensaje (*message authentication code*)
MHL	Enlace móvil de alta definición (*mobile high-definition link*)
NFC	Comunicación en el campo cercano (*near field communication*)
NGN	Redes de la próxima generación (*next generation networks*)
NLOS	Sin visibilidad directa (*non-line of sight*)
OBD	Diagnóstico a bordo (*on board diagnostics*)
OBU	Unidad a bordo (*on-board unit*)
PKI	Infraestructura de clave pública (*public-key infrastructure*)
QoS	Calidad de servicio (*quality of service*)
RSU	Unidad vial (*road-side unit*)
SCMS	Sistema de gestión de credenciales de seguridad (*security credential management system*)
SHA	Algoritmo de troceado seguro (*secure hash algorithm*)
STI	Sistema de transporte inteligente
USB	Bus serie universal (*universal serial bus*)
V2I	Vehículo a infraestructura (*vehicle-to-infrastructure*)
V2D	Vehículo a dispositivo nómada (*vehicle-to-nomadic device*)
V2P	Vehículo a peatón (*vehicle-to-pedestrian*)
V2V	Vehículo a vehículo (*vehicle-to-vehicle*)
V2X	Vehículo a entorno (*vehicle-to-everything*)
VGP	Plataforma de pasarela de vehículo (*vehicle gateway platform*)
VRU	Usuarios vulnerables de la vía pública (*vulnerable road user*)
WAVE	Acceso inalámbrico en entornos vehiculares (*wireless access in vehicular environments*)
WiFi	Fidelidad inalámbrica

5 Convenios

Ninguno.

6 Comunicación entre el vehículo y su entorno (V2X)

6.1 Generalidades

Los sistemas de transporte inteligentes (STI) comprenden una amplia gama de tecnologías de la información y la comunicación diseñadas para mejorar la seguridad y la eficacia de los sistemas de transporte. En los últimos años este sector ha experimentado una importante evolución, sobre todo en lo que respecta a los sistemas de comunicación en vehículos.

Los sistemas de comunicación vehiculares permiten intercambiar datos entre vehículos, entre vehículos e infraestructuras y entre vehículos y dispositivos nómadas. Se intercambian datos como la posición actual, la velocidad del vehículo y las alertas generadas por los sensores a bordo. Además, las unidades viales (RSU, *road-side units*) pueden servir de enlace de comunicación con un sistema de control del tráfico que capte y distribuya las alertas sobre los peligros en torno a los vehículos. Sin embargo, si no se protege adecuadamente su seguridad, los STI pueden resultar peligrosos para el tráfico y para la vida humana. Por consiguiente, es necesario abordar la seguridad de los STI a fin de poder desplegarlos con éxito y seguridad.

En la Figura 1 se muestra una visión general de la comunicación vehicular, que puede clasificarse en comunicación externa o interna con respecto al vehículo. En la red interna de un vehículo, conocida como red intravehicular (IVN, *in-vehicle network*), participan componentes del vehículo, como los sensores y las unidades de control electrónicas (ECU, *electronic control units*). Las comunicaciones externas pueden clasificarse en cuatro categorías: V2V, V2I, V2D y V2P. Las unidades a bordo (OBU, *on-board units*) son unidades de comunicación inalámbrica integradas en los vehículos, mientras que las RSU son unidades de acceso inalámbrico situadas en la vía pública. Por infraestructura se entienden las RSU y las instalaciones de soporte, como los sistemas de gestión y control del tráfico y las autoridades de certificación (CA, *certification authority*). Las RSU pueden estar conectadas a las instalaciones de soporte mediante redes alámbricas o inalámbricas.

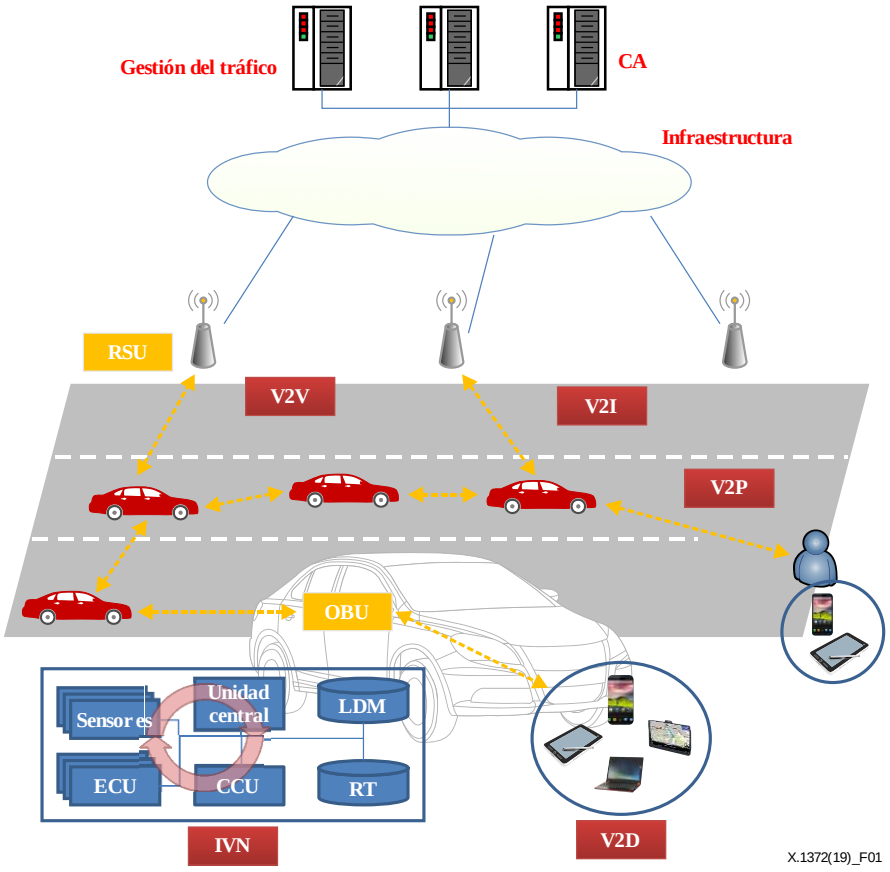


Figura 1 – Visión general de la comunicación vehicular

6.2 Comunicación vehículo a vehículo (V2V)

La comunicación vehículo a vehículo (V2V, *vehicle-to-vehicle*) es la transmisión inalámbrica de datos entre vehículos. El objetivo de la comunicación V2V es evitar accidentes mediante el envío y la compartición de información entre vehículos. En función de la implementación de la tecnología V2V, un vehículo puede recibir una alerta que le informe del posible riesgo de accidente. A continuación, el vehículo podrá tomar medidas preventivas, como frenar para perder velocidad. En la V2V, la comunicación en pelotón puede facilitar la conducción grupal mediante la compartición de información sobre la velocidad y las condiciones de la carretera. Además, puede recurrirse al balizaje para intercambiar información entre vehículos a fin de facilitar y asegurar la conducción. Con la ayuda de la comunicación V2V un vehículo puede recibir información sobre su entorno próximo a 360 grados.

Se han identificado las siguientes posibilidades de comunicación V2V:

– Propagación de alertas por V2V:

  En el caso de la propagación de alertas por V2V, se propaga un mensaje de alerta de un vehículo a otro. Por ejemplo, en caso de accidente de tráfico, se puede transmitir una alerta a todos los vehículos que se acercan al lugar del accidente, informándoles de que se dirigen hacia el lugar donde ha habido una colisión. Por otra parte, si un vehículo de emergencia, como un coche de policía, se acerca por detrás, se transmitirá un mensaje de alerta a todos los vehículos que estén por delante y en las cercanías, de tal manera que el vehículo de emergencia pueda aproximarse de forma segura a gran velocidad. En la Figura 2 se ilustra el caso en que se emite "hacia atrás" una alerta a los vehículos que se aproximan al lugar de un accidente; y en la Figura 3 se ilustra la emisión de una alerta "hacia delante" para avisar a los vehículos de que por detrás llega un vehículo de emergencia.

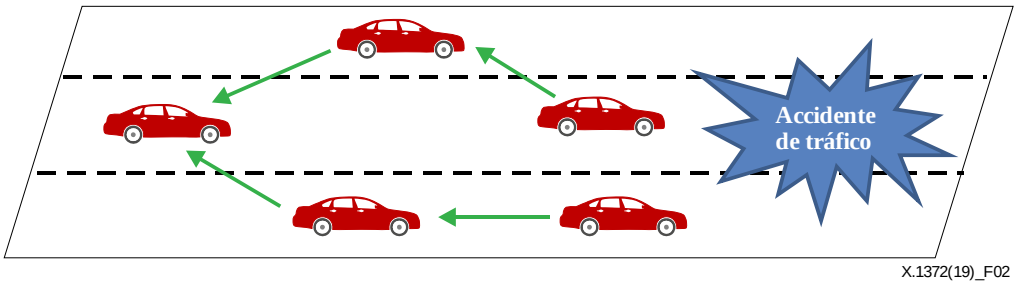


Figura 2 – Propagación de alertas por V2V – propagación hacia atrás

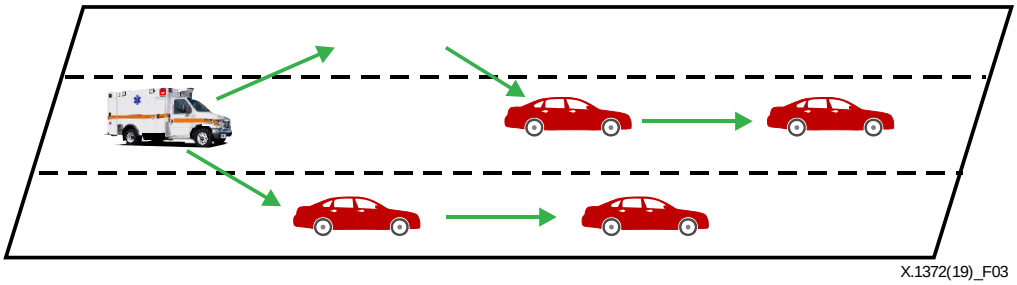


Figura 3 – Propagación de alertas por V2V – propagación hacia delante

– Comunicación en pelotón por V2V:

En el caso de la comunicación en pelotón por V2V, varios vehículos forman un grupo que pueden comunicarse entre sí dentro del grupo. Por ejemplo, los vehículos que tomen la misma ruta, al menos durante un tiempo, pueden formar un pelotón. Este grupo podrá comunicar información sobre el estado de los vehículos para contribuir a la conducción segura. En la Figura 4 se ilustra la comunicación en pelotón por V2V.

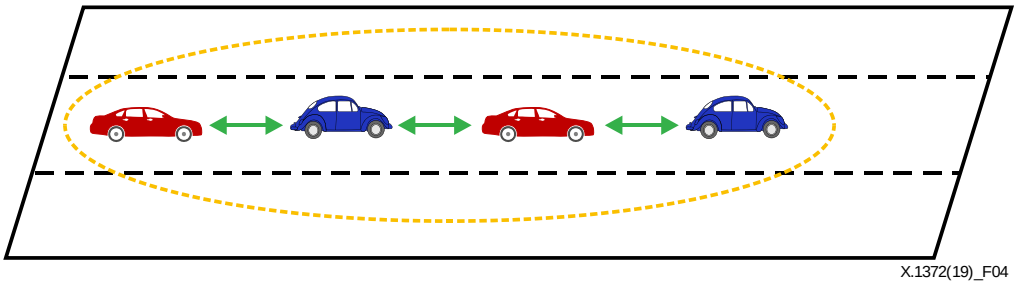


Figura 4 – Comunicación en pelotón por V2V

– Balizaje por V2V:

Cuando se realiza el balizaje por V2V, cada vehículo envía periódicamente información sobre su propio estado, a saber, la velocidad actual, la dirección y la posición, a los vehículos cercanos. En la Figura 5 se ilustra el balizaje por V2V.

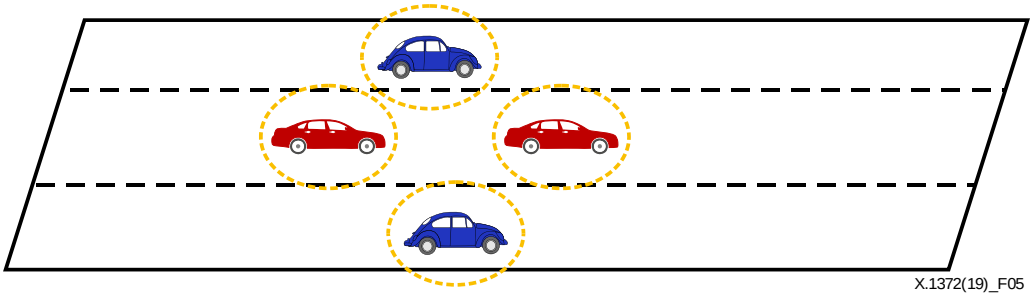


Figura 5 – Balizaje por V2V

6.3 Comunicación vehículo a infraestructura (V2I)

La comunicación vehículo a infraestructura (V2I, *vehicle-to-infrastructure*) es la transmisión inalámbrica de datos entre los vehículos y la infraestructura, por ejemplo, las unidades viales (RSU).

Se han identificado las siguientes posibilidades de comunicación V2I:

– Alerta por V2I:

La alerta por V2I permite la comunicación entre un vehículo y la infraestructura, como las RSU. Por ejemplo, en caso de accidente de tráfico en una intersección, la RSU puede enviar un mensaje de alerta a los vehículos que se acercan a la intersección. Otras alertas por V2I pueden avisar de la proximidad de vehículos en carriles de entrada, en giros a izquierda o derecha y en puntos de confluencia. En la Figura 6 se muestra un ejemplo de alerta por V2I.

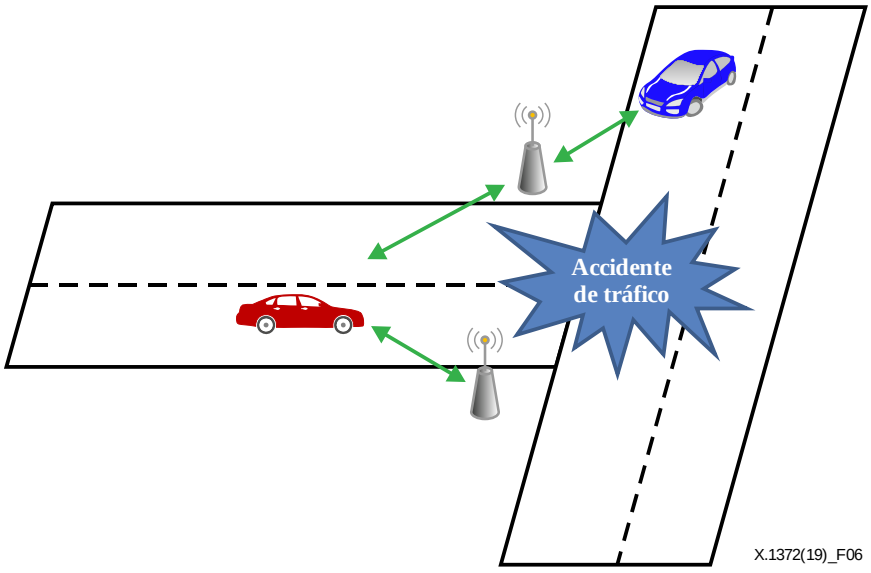


Figura 6 – Alerta por V2I

– Intercambio de información por V2I (incluida la V2V):

La información intercambiada por V2I puede comprender la señalización/información dentro del vehículo, información sobre la fase de señal y la temporización de los semáforos, datos de vehículos sonda, información de contabilidad (por ejemplo, peajes), información sobre las condiciones del firme/meteorológicas/de visibilidad e información sobre obras en la vía pública. Como ejemplos pueden citarse los siguientes:

- Descarga de datos de transporte básicos:

  En los STI algunos mensajes V2I pueden contener alertas. Para tratar esos mensajes generalmente el vehículo necesita un mapa de su localización o su destino y puede

necesitar información sobre las condiciones que rodean al vehículo en tiempo real. Esa información suele descargarse de la infraestructura, como las RSU.

- Datos para la eficacia del transporte:

  Con los STI los vehículos pueden comunicar ocasionalmente con la infraestructura a fin de obtener información sobre el tráfico, a saber, información sobre control temporal del tráfico, etc. Así, es posible saber dónde hay atascos para, entonces, optimizar la ruta con la ayuda de la infraestructura, por ejemplo, actualizando la ruta en un navegador con conectividad de red móvil. De este modo es posible aumentar la eficacia de los vehículos gracias a la comunicación V2I. Otro ejemplo puede ser el de la infraestructura que actualiza la información sobre el tráfico a partir de los mensajes recibidos de los vehículos por comunicación V2I. En la Figura 7 se ilustra el intercambio de información por V2I.

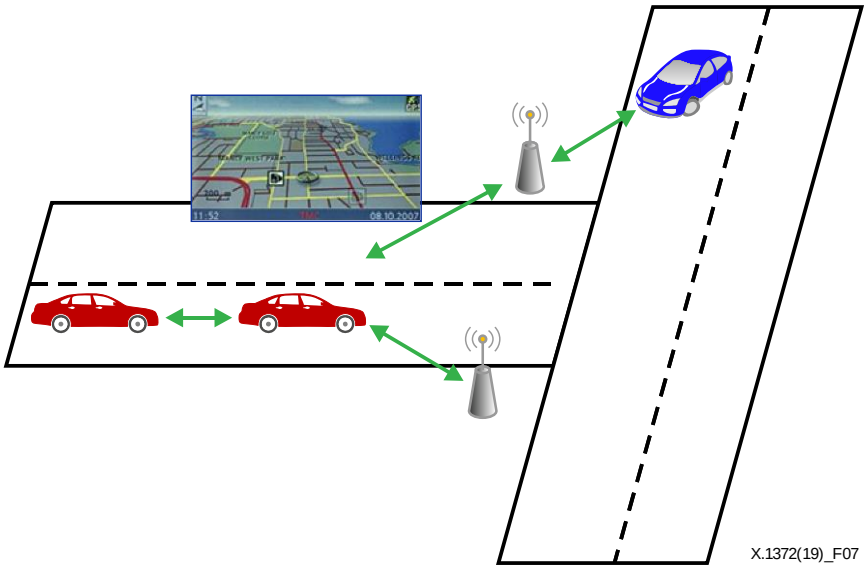


Figura 7 – Intercambio de información por V2I

6.4 Comunicación vehículo a dispositivo nómada (V2D)

Gracias a la tecnología de comunicación vehículo a dispositivo nómada (V2D, *vehicle to nomadic device*), los vehículos pueden conectarse a dispositivos como los teléfonos inteligentes, los ordenadores portátiles y los sistemas de navegación dentro del vehículo ya sea mediante una arquitectura abierta con una interfaz normalizada al bus de red de área del controlador (CAN, *controller area network*) del vehículo o empleando una pasarela que ejerza de intermediario para las solicitudes/respuestas entre el dispositivo nómada y el sistema que se ejecuta en el vehículo. Con un teléfono inteligente o dispositivo móvil pueden activarse a distancia funciones para identificar y gestionar la información sobre el estado del vehículo, como el mantenimiento de las piezas. Además, se espera que surjan nuevos y convenientes servicios.

Tomemos por ejemplo la planificación de un viaje, en la que el conductor elige un destino en un dispositivo nómada que, a su vez, planifica una ruta tomando distintas informaciones de diferentes fuentes, como los horarios del transporte público (tren, metro, autobús, etc.) e información de tráfico en tiempo real. El vehículo sigue la ruta planificada, modificándola si se dan cambios puntuales en las condiciones del tráfico. El dispositivo nómada no sólo decide qué maniobras hay que realizar y las ejecuta, sino que también reacciona a las condiciones del tráfico local, por ejemplo, seguir a otros vehículos, evitar obstáculos, cambiar de carril y detenerse en los semáforos. Este dispositivo nómada puede conectarse a las redes intravehiculares. Por consiguiente, es posible que un atacante pueda acceder a los sistemas internos del vehículo. En el caso de las amenazas a la seguridad por Bluetooth, es posible ejecutar códigos malignos a través de aplicaciones en los teléfonos inteligentes conectados

al vehículo. Los sistemas de audio, vídeo y navegación (AVN, *audio, video, and navigation*) intravehiculares son vulnerables a los ataques de software privado (*firmware*) a través de almacenes de multimedios y pueden fácilmente exponerse al pirateo a través del sistema de posicionamiento global (GPS, *global positioning system*) o canales de radio por satélite. Es necesario controlar los ataques a través de dispositivos nómadas para evitar los riesgos para la seguridad del vehículo.

A continuación se examinan los dos tipos de comunicación V2D diferentes:

– Comunicación V2D por enlaces indirectos:

  Los vehículos y los dispositivos nómadas pueden comunicar mediante enlaces indirectos. Por comunicación por enlaces indirectos se entiende que se recurre a equipos terceros, como puntos de acceso y encaminadores, para comunicar un nodo extremo con otro. Los teléfonos celulares y teléfonos inteligentes utilizan tecnologías de banda ancha móvil inalámbrica como la evolución a largo plazo, (LTE, *long term evolution*), fidelidad inalámbrica (Wi-Fi), etc. Cada vez se utiliza más Wi-Fi para comunicar los teléfonos inteligentes y los vehículos. Las tecnologías 5G también son un canal de comunicación clave para estos enlaces indirectos.

– Comunicación V2D por enlaces directos:

  Los vehículos y los dispositivos nómadas pueden comunicar mediante enlaces directos sin intervención externa entre ellos o utilizando tecnologías de comunicación inalámbrica como Bluetooth, ZigBee y comunicación en el campo cercano (NFC, *near field communication*).

  Los vehículos y los dispositivos nómadas también pueden comunicar por enlaces alámbricos. Por ejemplo, un dispositivo nómada puede conectarse a un vehículo mediante un acceso físico, como un bus serie universal (USB, *universal serial bus*), un enlace de alta definición móvil (MHL, *mobile high-definition link*) o una interfaz multimedios de alta definición (HDMI, *high-definition multimedia interface*). La norma de diagnóstico a bordo II (OBD-II, *on-board diagnostics II*) especifica las interfaces de diagnóstico y presenta una lista de posibles parámetros de vehículos y procedimientos para la transmisión de datos.

  La comunicación vehículo a peatón (V2P, *vehicle-to-pedestrian*) puede considerarse un caso particular de la comunicación vehículo a dispositivo nómada (V2D), pues el vehículo comunica con un dispositivo nómada asociado a un peatón.

  La V2P tiene aplicaciones para un amplio conjunto de usuarios vulnerables de la vía pública (VRU, *vulnerable road users*), incluidos los usuarios de la vía pública no motorizados, como los peatones y los ciclistas, así como los motociclistas y las personas con discapacidad o movilidad reducida.

  Dado el elevado número de accidentes de tráfico en los que están implicados los VRU, los STI proponen soluciones para aumentar la seguridad vial mediante la captación de datos de sensores y conceptos tales como la percepción y habilitación del intercambio de información entre vehículos y peatones. Cabe destacar que la comunicación V2P no sólo alertará al conductor del vehículo de que se acerca un peatón y debe parar, sino que también alertará al teléfono móvil del peatón para que éste le notifique la proximidad de un vehículo.

  Los STI pueden detectar a los VRU y contribuir a evitar colisiones entre vehículos y VRU. En la Figura 8 se muestra el caso en que un peatón se encuentra en la línea de visibilidad directa (LOS, *line of sight*) del conductor y en la Figura 9 el caso donde no hay visibilidad directa (NLOS, *non-line of sight*) entre el peatón y el conductor. Ambos ejemplos sirven para demostrar como los STI pueden mejorar la seguridad vial del VRU.

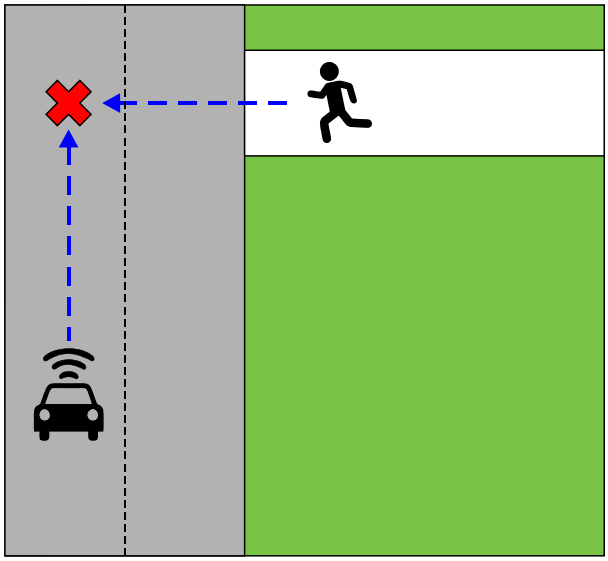


Figura 8 – Visibilidad directa

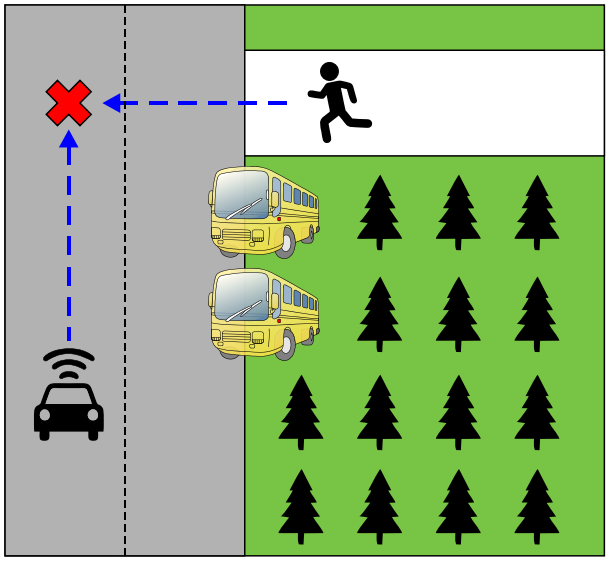


Figura 9 – Sin visibilidad directa

- Visibilidad directa del peatón (LOS):

  Como se ve en la Figura 8, los sensores activos, como los radares, los sensores de ultrasonidos, los telémetros laser y las cámaras de vídeo utilizan métodos de visión informática para detectar a los peatones cuando éstos son visibles desde el vehículo. Cuando un peatón se acerca, el vehículo en movimiento detecta al peatón y puede tomar una decisión clave. Al mismo tiempo, el vehículo puede indicar al teléfono celular del peatón que le alerte del posible peligro.

- Sin visibilidad directa del peatón (NLOS):

  La capacidad de detectar a los peatones está limitada por el campo visual de los sensores. En la Figura 9 la visión del peatón está obstaculizada por obstáculos, como árboles y autobuses aparcados. Sin embargo, gracias a la comunicación vehicular se puede anunciar y divulgar información más allá del campo visual del sensor. Una vez que el vehículo ha recibido la alerta, actualiza su mapa dinámico local (LDM, *local dynamic map*) y evalúa la gravedad de la situación para tomar una decisión. Al mismo tiempo, el teléfono celular del peatón recibe una notificación de alerta.

7 Amenazas identificadas

7.1 Amenazas a la confidencialidad

En la Figura 10 se ilustran las amenazas a la confidencialidad descritas en esta cláusula.

– Escucha clandestina:

  Un atacante puede inspeccionar los mensajes V2V (es decir, leerlos y/o guardarlos) de los vehículos cercanos y los mensajes V2I de las RSU y analizar la información del tráfico mediante el procesamiento de los mensajes inspeccionados.

  Un atacante puede inspeccionar los mensajes V2D entre una unidad central de comunicación y un dispositivo nómada para, entonces, analizar la información dinámica del vehículo, como su localización y velocidad.

  Un atacante puede inspeccionar los mensajes V2P y dirigir intencionalmente a los peatones hacia situaciones viales peligrosas.

– Fuga de información de identificación personal:

  Un atacante puede analizar la información para descubrir quién es el propietario del vehículo gracias a los mensajes V2X y rastrear la localización de una persona concreta a lo largo del camino.

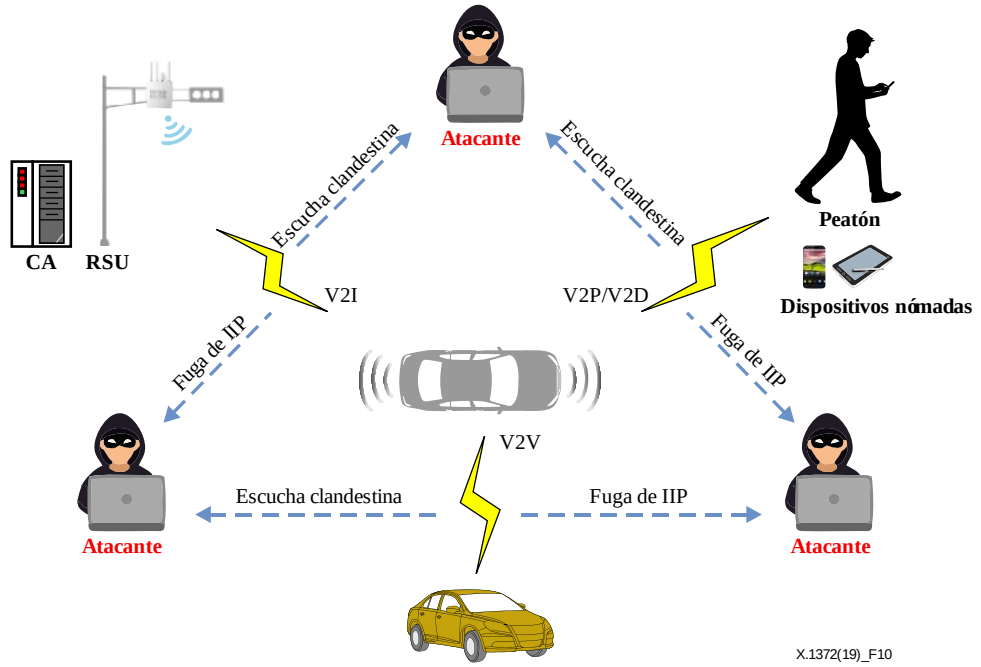


Figura 10 – Amenazas a la confidencialidad

7.2 Amenazas a la integridad

En la Figura 11 se ilustran las amenazas a la integridad descritas en esta cláusula.

– Manipulación de mensajes de encaminamiento:

  Un nodo intermedio maligno modifica los mensajes de encaminamiento y los vehículos reciben información falsa.

– Manipulación de información de credenciales:

  Por manipulación de credenciales se entiende la modificación de la clave privada o el ID (identificador) del vehículo de manera que el atacante puede utilizar la información de credenciales de otro vehículo sin autorización.

– Manipulación de información de sensores:

  Un atacante puede modificar la dirección física de un módulo de comunicación o manipular la información de la ECU, por ejemplo, del sensor de velocidad. Además, los vehículos llevan incorporados, como equipos de ayuda a la conducción, muchos sensores, como radares y cámaras. Es posible comunicar a otras OBU o RSU datos de sensores falsos, incluidas la latitud, la longitud, la elevación, la velocidad, la dirección, el ángulo del volante y la aceleración, y esos datos manipulados pueden causar problemas en el tráfico. Por ejemplo, un valor de aceleración falso puede hacer que los vehículos vecinos activen sus luces de freno de emergencia electrónicas (EEBL, *electronic emergency brake lights*) para reducir las posibilidades de colisión múltiple, aunque en realidad las condiciones del tráfico sean buenas.

– Manipulación de aplicaciones en dispositivos nómadas:

  Las aplicaciones manipuladas pueden tener efectos nocivos en los vehículos a través de la interfaz de comunicación V2D. por ejemplo, una aplicación manipulada puede forzar al dispositivo nómada a enviar una gran cantidad de mensajes inocuos al vehículo; esto se conoce como inundación de mensajes. También es posible que una aplicación manipulada

inyecte código maligno en una OBU y envíe un mensaje que necesite muchos recursos de computación. Otra posibilidad es que envíe un gran número de mensajes de tamaño muy superior a la capacidad de almacenamiento disponible de la OBU.

– Ataque por repetición:

El atacante puede interceptar los mensajes V2V de los vehículos cercanos y los mensajes V2I de las RSU. Posteriormente, el atacante reproduce esos mensajes o informaciones con fines malignos.

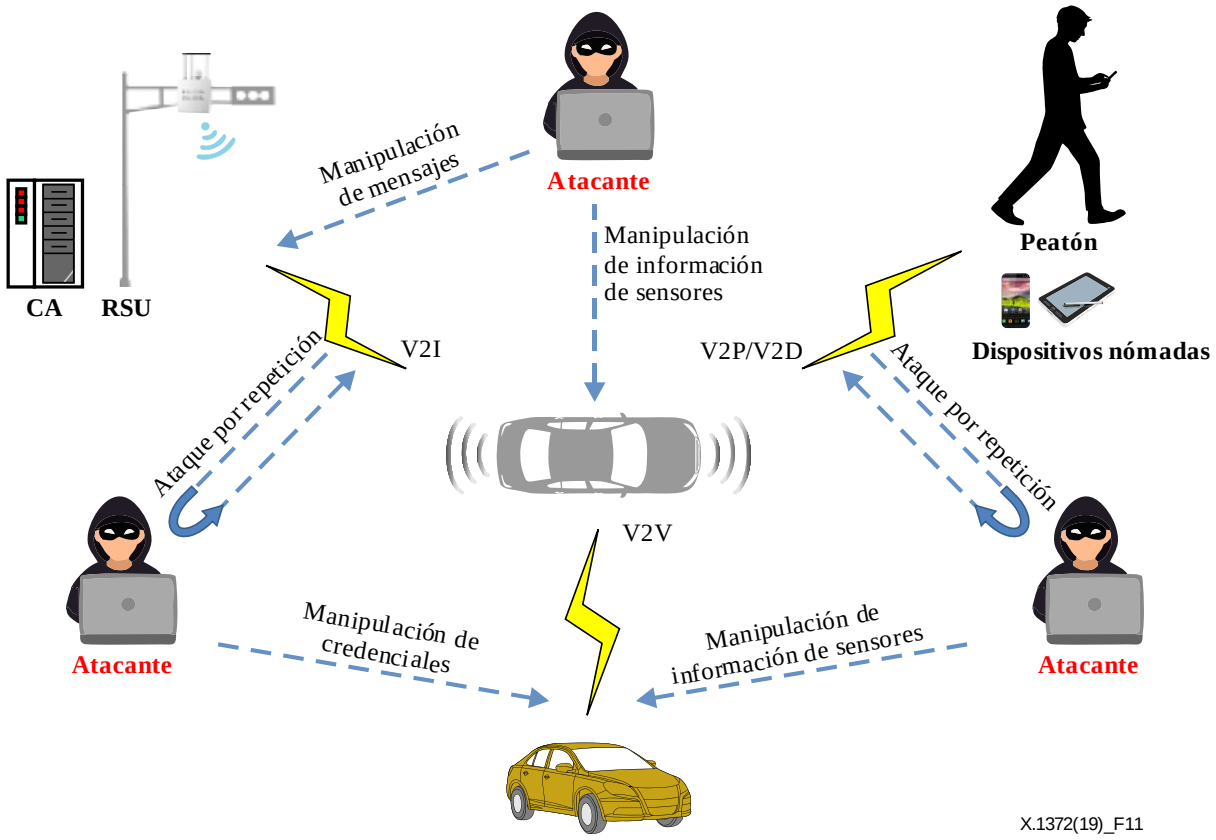


Figura 11 – Amenazas a la integridad

7.3 Amenazas a la disponibilidad

En la Figura 12 se ilustran las amenazas a la disponibilidad descritas en esta cláusula.

– Interferencia deliberada y ataque de denegación de servicio distribuida (DDoS, *distributed denial of service*) de un canal de comunicación V2X:

Un atacante puede enviar múltiples mensajes inútiles; esta técnica se conoce como inundación de mensajes. Dentro de esta categoría de ataques se cuenta el simple reenvío de un mensaje específico por un nodo de encaminamiento.

– Ataque DDoS de una OBU:

El atacante puede inyectar códigos malignos en una OBU y enviar mensajes que exigen notables recursos de computación. El atacante puede asimismo enviar numerosos mensajes cuyo tamaño acumulado supera el de la capacidad de almacenamiento de la OBU. La actualización frecuente del software sin autorización es un ejemplo concreto de ataque grave de este tipo.

– Ataque de temporización:

Un ataque de temporización consiste, por ejemplo, en retrasar la entrega de mensajes de seguridad a otros vehículos de modo que se impida la adecuada ejecución de servicios de comunicación V2X, como la radiodifusión de mensajes de alerta.

– Pirateo de sensores:

Es posible piratear los sensores y causar fallos que originen valores malignos. En general hay dos tipos de fallos de sensores: fallos transitorios y fallos permanentes. Los fallos transitorios pueden darse durante el funcionamiento normal del sistema y desaparecen rápidamente. De hecho, la mayoría de sensores sigue un modelo de fallo transitorio que limita la cantidad de tiempo durante el cual dan mediciones erróneas. Por ejemplo, es habitual que el GPS pierda la conexión con los satélites (o reciba señales ruidosas), sobre todo en ciudades con edificios altos. Del mismo modo, un sensor que transmite datos por una red congestionada (por ejemplo, con protocolo TCP/IP con retransmisiones) puede no llegar a dar las mediciones a tiempo, por lo que, cuando llegan los mensajes, la información que contienen es incorrecta. Sin embargo, por su escasa duración, los fallos transitorios no deben considerarse una amenaza para la seguridad del sistema.

Por otra parte, los fallos permanentes son defectos del sensor que persisten durante un periodo de tiempo más largo y pueden afectar gravemente al funcionamiento del sistema. Por ejemplo, un sensor puede sufrir daños físicos que generen un sesgo permanente de las mediciones que efectúa. En tal caso, a menos que el software pueda corregir el fallo, será mejor para el sistema descartar por completo ese sensor.

Dependiendo de cuál sea el objetivo del atacante, los ataques a las mediciones de los sensores pueden manifestarse como fallos transitorios o permanentes. Cada uno de ellos ofrece ventajas e inconvenientes al atacante. Hacer que un sensor se comporte como si estuviera en fallo transitorio puede impedir que se descubra la identidad del atacante, pero limita sus capacidades, mientras que un ataque prolongado semejante a un fallo permanente puede ser más potente, pero detectarse más rápidamente.

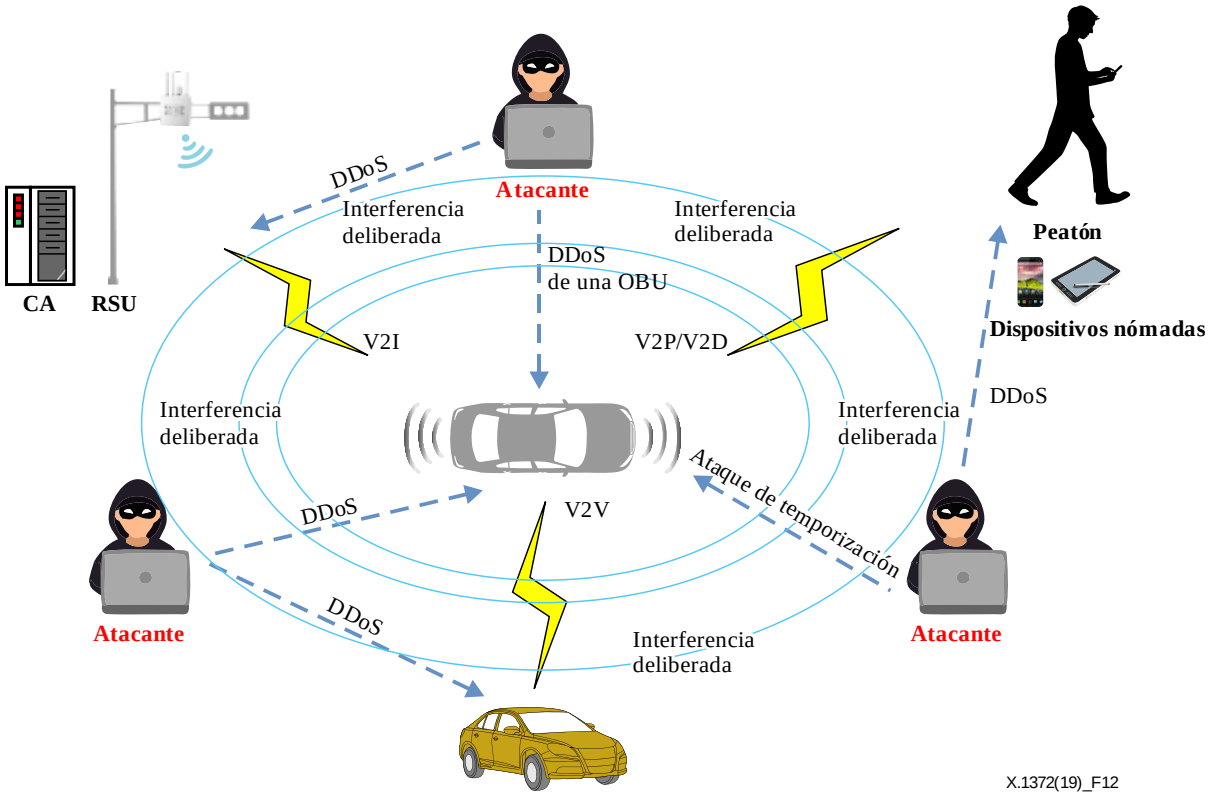


Figura 12 – Amenazas a la disponibilidad

7.4 Amenazas al no repudio

En la Figura 13 se ilustran las amenazas al no repudio descritas en esta cláusula.

– Manipulación de la base de datos de certificación:

  Un atacante puede manipular la base de datos de seudónimos de la CA y modificar la relación entre un certificado a largo plazo y un certificado de seudónimo a corto plazo.

– Acceso no autorizado a las credenciales:

  Un atacante puede acceder a las claves privadas y certificados sin autorización. Si se expone la clave privada, resulta imposible garantizar el no repudio del vehículo, la RSU y el dispositivo nómada.

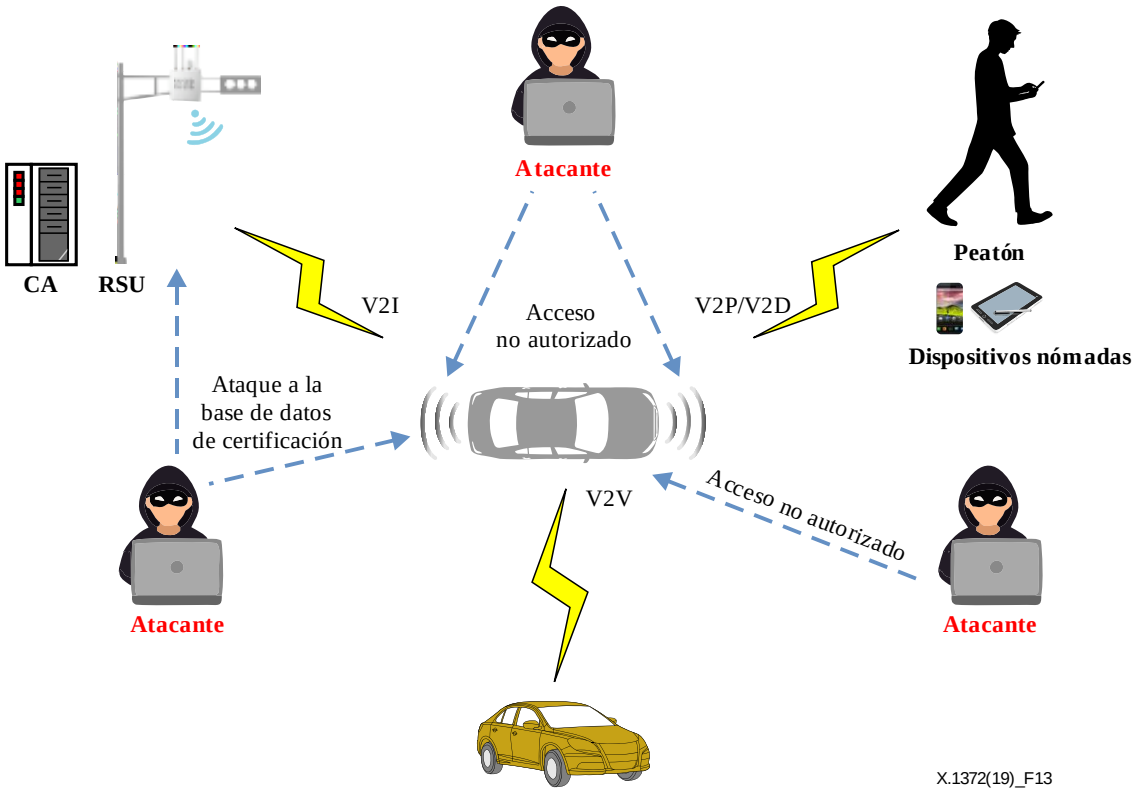


Figura 13 – Amenazas al no repudio

7.5 Amenazas a la autenticidad

En la Figura 14 se ilustran las amenazas a la autenticidad descritas en esta cláusula.

– Ataque por modificación del LMD y la tabla de encaminamiento:

  Un atacante puede falsificar la información del GPS de un vehículo y modificar su información geoespacial original.

– Ataque por suplantación:

  El atacante puede aparentar ser otra entidad tras haber robado la información de identidad de esa entidad. El atacante recibirá entonces los mensajes que normalmente se envían a la otra entidad y también podrá enviar mensajes como si hubieran sido generados normalmente por la otra entidad. Por ejemplo, si la otra entidad es un vehículo de emergencia, el atacante podrá enviar un mensaje a los demás vehículos cercanos que diga, por ejemplo, "Soy un vehículo de emergencia. Apártese de mi camino."

  También es posible que el atacante envíe una falsa señal de funcionamiento erróneo en nombre de un vehículo inocente de modo que la CA revoque el certificado del vehículo inocente.

– Ataque Sibila:

  Un ataque Sibila es aquel en el que, por ejemplo, un vehículo simula ser múltiples vehículos utilizando múltiples ID de vehículo.

– Ataque por análisis de seudónimo:

  Un atacante puede analizar la relación entre los ID del vehículo y los seudónimos a fin de encontrar los distintos seudónimos utilizados para el mismo vehículo.

– Manipulación de la base de datos de certificación:

  Un atacante puede manipular la base de datos de seudónimos de la CA y, posteriormente, modificar la relación entre un certificado a largo plazo y un certificado de seudónimo a corto plazo.

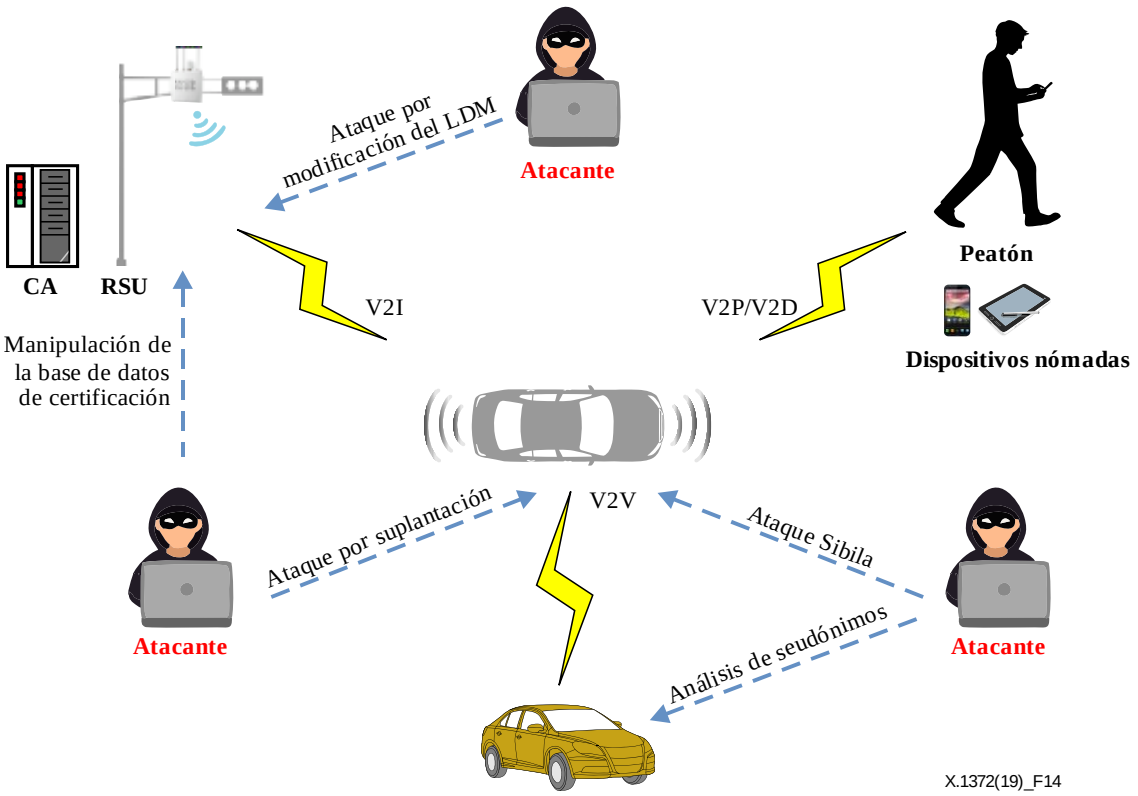


Figura 14 – Amenazas a la autenticidad

7.6 Amenazas a la imputabilidad

En la Figura 15 se ilustran las amenazas a la imputabilidad descritas en esta cláusula.

– Duplicación no autorizada de un dispositivo nómada:

  Para algunos servicios concretos, como el diagnóstico del vehículo, por ejemplo, dispositivos nómadas autorizados pueden acceder a la unidad central de comunicación del vehículo. No obstante, si dispositivos malignos copian esa autorización, como puede pasar si, por ejemplo, otro dispositivo maligno ha utilizado la cuenta de registro del dispositivo autorizado, los dispositivos malignos pueden acceder a la unidad de comunicación. En ese caso, un dispositivo nómada no autorizado podría manipular la unidad central de comunicación de un vehículo.

– Duplicación no autorizada de un vehículo y una RSU:

  Una vez que el atacante obtiene (duplica) los ID del vehículo y de la RSU, éstos pierden su imputabilidad.

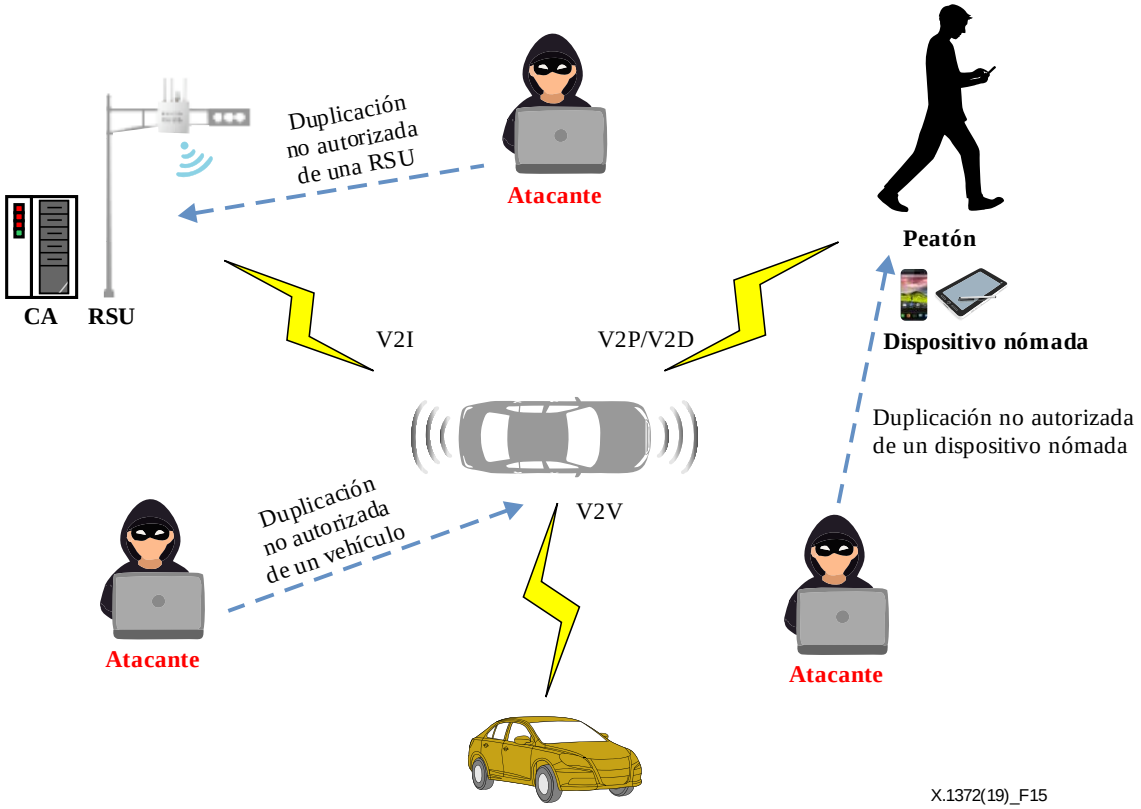


Figura 15 – Amenazas a la imputabilidad

7.7 Amenazas a la autorización

En la Figura 16 se ilustran las amenazas a la autorización descritas en esta cláusula.

– Acceso no autorizado a la información de seguridad de un vehículo:

  Si no se controla la autorización, un usuario o aplicación malignos pueden controlar un vehículo sin autorización. Por ejemplo, la aplicación que reproduce música por el altavoz de un vehículo no debería estar autorizada a acceder a información de seguridad, como la velocidad del vehículo o el estado del freno.

  Un atacante no autorizado puede también manipular, borrar y reescribir los datos de seguridad del vehículo, incluidos parámetros tales como el umbral de freno, el airbag de emergencia y el registro del sistema.

  En el caso de los vehículos eléctricos, los atacantes no autorizados pueden manipular los parámetros de configuración de las funciones de carga del vehículo.

– Acceso no autorizado a determinadas funciones de un vehículo mediante dispositivos nómadas:

  Es fundamental definir las funciones de control de acceso para los dispositivos nómadas que se conectan al vehículo. Normalmente los dispositivos nómadas se utilizan como una herramienta de audio, vídeo y navegación del vehículo. También es posible mostrar el contenido de los dispositivos nómadas en la unidad multimedios del vehículo. La ejecución de funcionalidades no autorizadas, como la comunicación con una pasarela central, con esos dispositivos nómadas pueden tener graves consecuencias para la seguridad.

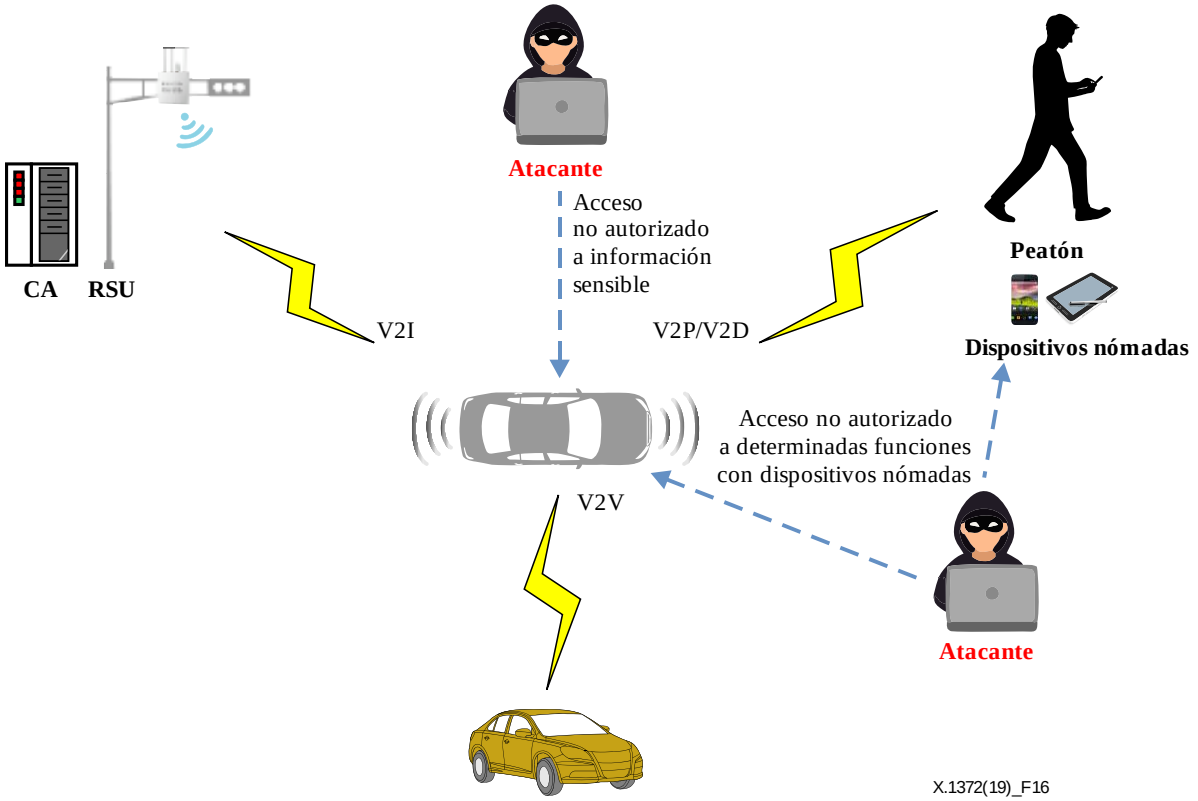


Figura 16 – Amenazas a la autorización

8 Requisitos de seguridad

En esta cláusula se describen los requisitos de seguridad de la comunicación V2X. Las cláusulas 8.1 a 8.7 describen los requisitos de seguridad en las comunicaciones V2X, y la cláusula 8.8 proporciona más detalles sobre estos requisitos.

8.1 Confidencialidad

Una entidad no autorizada no debe poder revelar los mensajes entre vehículos, entre vehículos y la infraestructura, entre vehículos y dispositivos nómadas, y entre vehículos y peatones.

Una entidad no autorizada no debe poder analizar la identificación de una persona gracias a la información de identificación personal (IIP) de los mensajes, como el emplazamiento o la ruta que sigue una persona concreta.

8.2 Integridad

Los mensajes enviados desde y hacia un vehículo, una RSU o un dispositivo nómada deben estar protegidos contra la modificación o la supresión no autorizadas.

8.3 Disponibilidad

Una entidad debe poder enviar y recibir mensajes con la latencia adecuada. Por ejemplo, un mensaje de alerta de colisión frontal debe transmitirse al vehículo antes de que éste llegue al punto del accidente. Si el mensaje de alerta no puede entregarse a ese vehículo por un ataque de interferencia deliberada, la aplicación de seguridad V2V/V2I podría revelarse inútil.

Una entidad debe poder procesar la información intercambiada en tiempo real, para lo que se necesita la implementación de algoritmos criptográficos ligeros y con poca tara.

8.4 No repudio

Una entidad no debe poder negar que ha enviado un mensaje. Este requisito puede implementarse con firmas digitales en los sistemas de comunicación V2X.

8.5 Autenticidad

Entidades tales como las OBU y las RSU en el entorno de comunicación V2V/V2I deben poder demostrar la propiedad autorizada de un ID legítimo. Este requisito se conoce como autentificación de entidad. También es necesario entre un vehículo y un dispositivo nómada.

En el caso de la comunicación grupal, el vehículo no necesita demostrar su ID, sino que debe demostrar que es un miembro auténtico del grupo. Este requisito se denomina autentificación de atributo.

8.6 Imputabilidad

Toda entidad debe poder detectar y/o impedir comportamientos indebidos de las OBU o los sensores de los vehículos mediante verificación de sus datos.

Por ejemplo, una OBU puede verificar parte de la información recibida en un mensaje para comprobar la veracidad de los datos cinemáticos recibidos en un mensaje anterior. Si los datos de posición del último mensaje recibido muestran cambios imposibles en el comportamiento dinámico del vehículo, es posible que se trate de un comportamiento indebido de otra entidad. En tal caso, la información puede filtrarse o ignorarse.

8.7 Autorización

Es fundamental definir un control de acceso y autorización para las diferentes entidades. Se han de aplicar normas específicas para permitir o denegar el acceso a entidades específicas y/o permitir o no la utilización de ciertas funciones o datos.

8.8 Aplicabilidad de los requisitos de seguridad V2X

En el Cuadro 1 se enumeran los requisitos de seguridad descritos en las cláusulas 8.1 a 8.7, y su aplicabilidad a las diversas formas de comunicaciones V2X.

Cuadro 1 – Requisitos de seguridad para la comunicación V2X

	Propagación de alertas por V2V	**Comunicación en pelotón por V2V**	**Balizaje por V2V**	**Alertas por V2I**	**Intercambio de información por V2V/V2I**	**Comunicación V2D**	**Comunicación V2P**
Confidencialidad (general)	–	O	–	–	O	O	O
Confidencialidad (IIP)	O	O	O	▲	O	O	O
Integridad	O	O	O	O	O	O	O
Disponibilidad	O	O	O	O	O	▲	O
No-repudio	O	O	O	O	O	O	O
Autenticidad	O	▲	O	O	O	O	O
Imputabilidad	O	O	O	O	O	O	O
Autorización	–	O	–	–	O	O	–
O: Obligatorio, –: No obligatorio, ▲: parcialmente obligatorio							

Para la propagación de alertas por V2V no se exige obligatoriamente la confidencialidad, pues los mensajes intercambiados entre los vehículos contienen información pública, como los accidentes de tráfico ocurridos o la proximidad de vehículos de emergencia. Los mensajes de alerta propagados por V2V no contienen información relativa a la autorización.

Para la comunicación en pelotón por V2V se exige parcialmente la autentificación del vehículo, lo que supone que no es necesario que cada vehículo autentifique a todos y cada uno de los vehículos del grupo. Por autentificación de entidad se entiende el proceso mediante el cual se garantiza a una entidad la identidad de las demás entidades participantes en la comunicación. Sin embargo, en la comunicación en pelotón por V2V los vehículos no han de autentificar con exactitud a todas las entidades del grupo. En ese caso basta con demostrar que los vehículos son miembros del grupo. Dicho de otro modo, lo que se garantiza no es la identidad de los vehículos, sino su pertenencia al grupo. Este tipo de autentificación puede denominarse autentificación de atributo. Los mensajes intercambiados en este caso sí tienen información de autorización, por ejemplo, líder del pelotón o miembro del pelotón.

En el balizaje por V2V la información radiodifundida debe estar protegida contra la modificación y la supresión no autorizadas. Sin embargo, si el mensaje no contiene la información de identificación del vehículo, no es necesario que esté encriptado. Además, la autorización no es obligatoria para el balizaje por V2V, pues la información radiodifundida no se utilizará para ejercer control alguno.

En el caso de las alertas por V2I, la información intercambiada entre el vehículo y la infraestructura, por ejemplo, una RSU, suele ser información de tráfico del dominio público, motivo por el que en este caso no se exige la confidencialidad. La obligación parcial de protección de la IIP en las alertas por V2I implica que el vehículo necesita la protección de la IIP, pero no la RSU. Si el conductor está vinculado al vehículo, también será necesario proteger la localización del vehículo y su historial de desplazamientos. Sin embargo, las RSU carecen de IIP, pues no están vinculadas a personas físicas.

En la comunicación V2D el dispositivo nómada se utiliza dentro del vehículo. Cuando el dispositivo nómada comunica con el vehículo, la disponibilidad no tiene la misma importancia que en el caso de la comunicación V2V, pues el número de dispositivos dentro del vehículo es inferior al de vehículos en carretera en entornos reales.

Para la comunicación V2P los dispositivos nómadas de los peatones o los VRU no pueden ejecutar funciones que exijan la autorización del vehículo.

9 Implementación segura de la comunicación V2X

En esta cláusula se presentan posibles implementaciones de la comunicación V2X que cumplen los requisitos de seguridad que se describen en la cláusula 8, a saber, confidencialidad, integridad, disponibilidad, etc. Se presentan brevemente los algoritmos criptográficos fundamentales adaptados a los entornos de comunicación vehicular y a continuación se explica cómo utilizarlos en las comunicaciones V2X, como las alertas de emergencia y la comunicación en pelotón.

9.1 Criptografía para la autentificación de entidades y la confidencialidad de los mensajes

La función de autentificación de entidades V2X puede ejecutarse con algoritmos de firma digital. La función de confidencialidad de mensajes puede implementarse con algoritmos criptográficos simétricos y de clave pública. En esta Recomendación se dan ejemplos de cómo implementar estas funciones. La adaptación y selección de mecanismos y parámetros, relacionados con las funciones de autentificación de entidades y de confidencialidad de mensajes, dependen de la política adoptada.

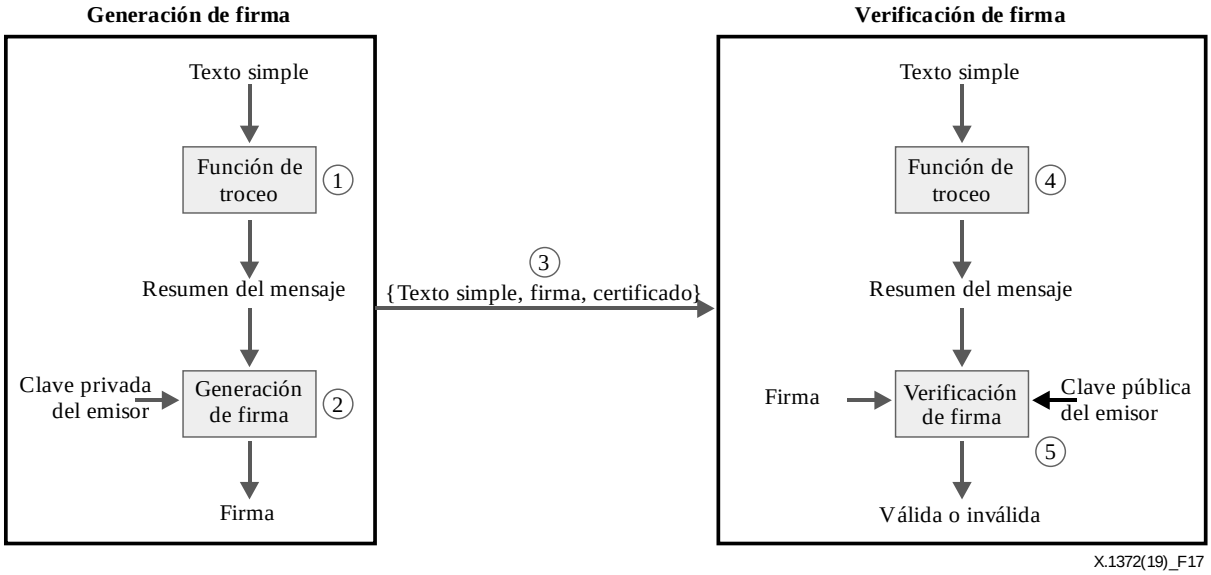


Figura 17– Generación y verificación de firmas

Un algoritmo de firma digital conlleva un proceso de generación de firma y un proceso de verificación de firma, como se muestra en la Figura 17. El signatario utiliza el proceso de generación para generar una firma digital en los datos. El usuario verificador recurre el proceso de verificación para comprobar la autenticidad de la firma. Cada signatario posee una clave pública y una clave privada. Como se ve en la Figura 17 la clave privada se utiliza en el proceso de generación de firma, mientras que la clave pública del signatario se utiliza en el proceso de verificación de firma.

Globalmente, el procesamiento de generación y verificación de firma es el siguiente:

– Paso 1: Con una función de troceo (como el algoritmo de generación numérica seguro SHA-256) se calcula un resumen de mensaje a partir del mensaje de texto simple. Por ejemplo, el resumen se calcula a partir de la versión del protocolo, el encabezamiento, la carga útil y la longitud de la cola.

– Paso 2: Se genera una firma del resumen del mensaje con la clave privada del emisor.

– Paso 3: El texto simple, la firma y el certificado del emisor se transmiten al receptor.

– Paso 4: El receptor calcula el resumen del mensaje con el texto simple recibido del emisor.

– Paso 5: El receptor calcula un valor de verificación utilizando el resumen del mensaje del paso 4, la firma recibida y la clave pública del emisor. Si el valor de verificación es idéntico al valor de la firma, la firma recibida es válida. Si el valor de verificación difiere del de la firma recibida, la firma es inválida.

En la comunicación V2X puede utilizarse como algoritmo de firma digital el algoritmo de firma digital de curva elíptica (ECDSA, *elliptic curve digital signature algorithm*).

Los algoritmos de encriptación se utilizan para garantizar la confidencialidad de los mensajes V2X. Se utilizan algoritmos de encriptación asimétrica, como el esquema de encriptación integrada de curva elíptica (ECIES, *elliptic curve integrated encryption scheme*), para transportar una clave de algoritmo de clave simétrica, como la norma de encriptación avanzada (AES, *advanced encryption standard*). En la Figura 18 se muestra el procedimiento de encriptación con ECIES, que utiliza las siguientes funciones:

– Acuerdo de claves (AK, *key agreement*): Función utilizada para la generación de un secreto compartido entre dos entidades.

– Función de derivación de claves (KDF, *key derivation function*): Mecanismo que produce un conjunto de claves a partir de información sobre las claves y otros parámetros optativos.

– Encriptación: Algoritmo de encriptación de clave simétrica.

– Código de autentificación de mensaje (MAC, *message authentication code*): Algoritmo de generación MAC.

En la Figura 18 se utiliza la siguiente notación:

– ***u***: Clave privada del emisor

– ***U***: Clave pública del emisor

– ***v***: Clave privada del receptor

– ***V***: Clave pública del receptor

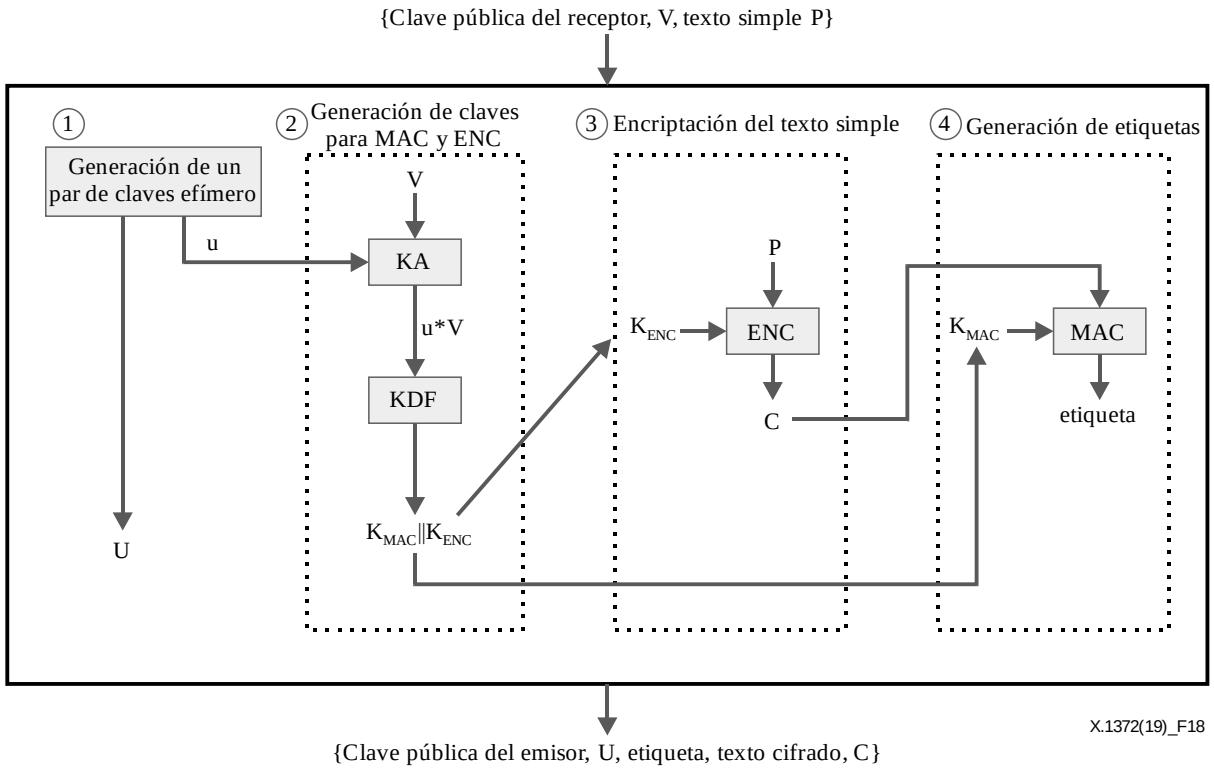


Figura 18 – Procedimiento de encriptación ECIES

Como se ve en la Figura 18, las entradas del procedimiento de encriptación son la clave pública del receptor, ***V***, y el texto simple, ***P***. Las salidas del procedimiento de encriptación son la clave pública del emisor, ***U***, la etiqueta y el texto cifrado, ***C***. El procedimiento de encriptación de mensajes consiste en los siguientes pasos:

– Paso 1: Generación de un par de claves efímero:

  El emisor genera la clave privada, ***u***, y la clave pública, ***U***. Se recomienda que la clave pública, ***U***, se genere nuevamente en cada operación de encriptación.

– Paso 2: Generación de claves para MAC y ENC:

  La función de acuerdo de claves (KA) genera un secreto compartido por la clave privada efímera del emisor, ***u***, y la clave pública del receptor, ***V***. La función de derivación de claves (KDF), basada en SHA-256, toma este secreto compartido para generar la concatenación de la clave de código de autentificación de mensajes (MAC) ($\boldsymbol{K_{MAC}}$) y la clave de encriptación ($\boldsymbol{K_{ENC}}$).

– Paso 3: Encriptación del texto simple:

  El texto simple, ***P***, se encripta con K_{ENC} utilizando algoritmos de encriptación simétrica.

  ECIES se utiliza para encriptar una clave simétrica para la encriptación de mensajes V2X utilizando el código de autentificación de mensaje en modo contador con concatenación de bloques cifrados (AES-CCM). Por consiguiente, el texto simple es en realidad la clave de encriptación para AES-CCM.

– Paso 4: Generación de etiquetas:

  Una función MAC con SHA-256 genera una etiqueta de texto cifrado, que es la clave simétrica de AES-CCM a fin de soportar la integridad del mensaje.

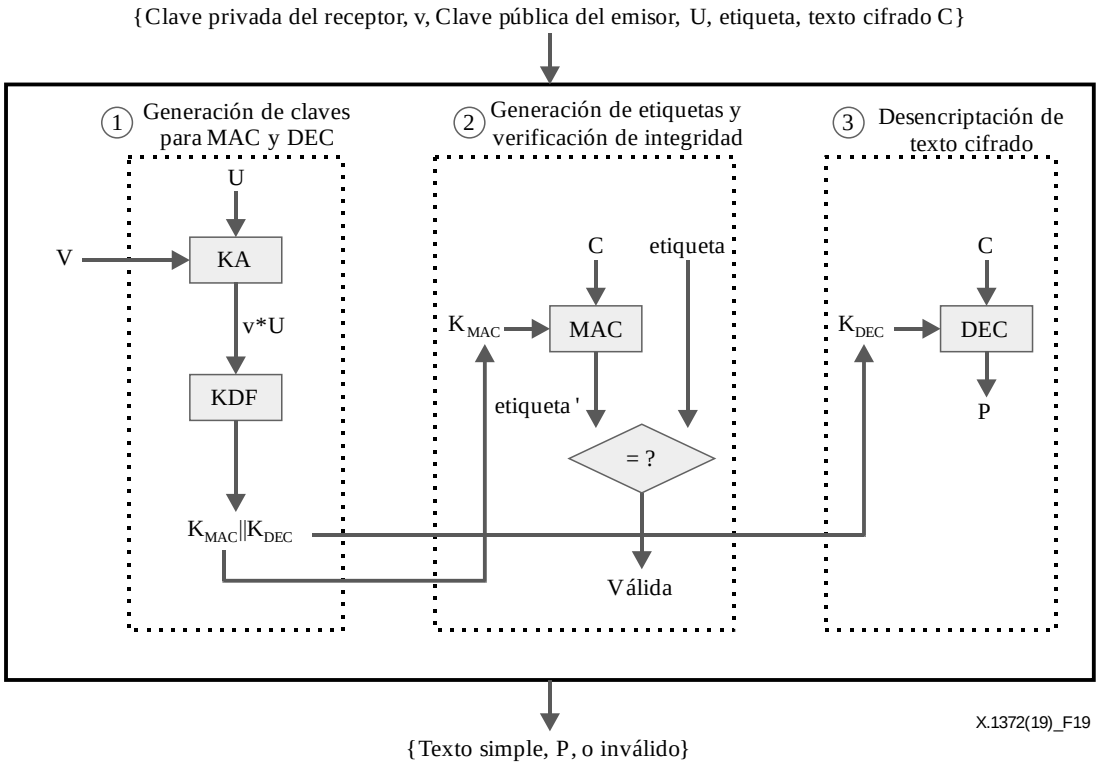


Figura 19 – Procedimiento de desencriptación

En la Figura 19 se describe el procedimiento de desencriptación de ECIES. Como se ve en la Figura 19, las entradas del procedimiento de desencriptación son la clave privada del receptor, ***v***, la clave pública del emisor, ***U***, la etiqueta y el texto cifrado, ***C***. Las salidas del procedimiento de desencriptación son el texto simple, ***P***, o los resultados de la prueba de integridad del mensaje. En la Figura 19 DEC denota el procedimiento de desencriptación del algoritmo de clave simétrica. El procedimiento de desencriptación de mensajes consiste en los siguientes pasos:

– Paso 1: Generación de claves para MAC y DEC:

  La función de acuerdo de claves (KA) genera un secreto compartido por la clave pública efímera del emisor, ***U***, y la clave privada del receptor, ***v***. La función de derivación de claves (KDF), basada en SHA-256, toma este secreto compartido para generar la concatenación de la clave de código de autentificación de mensaje (MAC), K_{MAC}, y la clave de desencriptación, K_{DEC}. Cabe señalar que K_{ENC} y K_{DEC} son los mismos valores en los algoritmos de clave simétrica.

– Paso 2: Generación de la etiqueta y verificación de la integridad:

  La función MAC genera una etiqueta de texto cifrado, ***C,*** recibido con K_{MAC}. La etiqueta calculada se compara con la etiqueta recibida. Si los valores no son idénticos, el mensaje recibido se descarta por fallo de la verificación de la integridad del mensaje.

– Paso 3: Desencriptación del texto cifrado:

  El texto cifrado, ***C***, se desencripta con K_{DEC} utilizando algoritmos de encriptación simétrica.

ECIES se utiliza para encriptar una clave simétrica para la encriptación de mensajes V2X utilizando AES-CCM. Por consiguiente, el texto simple es en realidad la clave de encriptación para AES-CCM.

9.2 Confidencialidad del mensaje para alertas de emergencia de seguridad vial

En la Figura 20 se ilustra un caso de uso genérico de alerta de emergencia. La ECU de freno envía un mensaje a la unidad de comunicación V2X del vehículo a través de su unidad central de comunicación (CCU). La aplicación de STI correspondiente de la unidad de comunicación V2X recibe el mensaje de la ECU de freno y genera un mensaje de alerta por V2X. El mensaje generado se envía a la capa de interconexión de redes y de transporte. El mensaje debe estar firmado o encriptado por la capa de seguridad. A continuación, la capa física envía el mensaje firmado o encriptado a un canal de comunicación inalámbrica. Gracias a este canal de comunicación inalámbrica el mensaje se transmite al receptor. Una vez recibido, la capa de seguridad verifica o desencripta el mensaje y, por último, lo pasa a la capa superior, es decir, la aplicación de STI correspondiente. La aplicación de STI puede actualizar el LDM o alertar al conductor a través de un dispositivo con interfaz humana y puede enviar un mensaje de control a la ECU de freno para reducir la velocidad del vehículo.

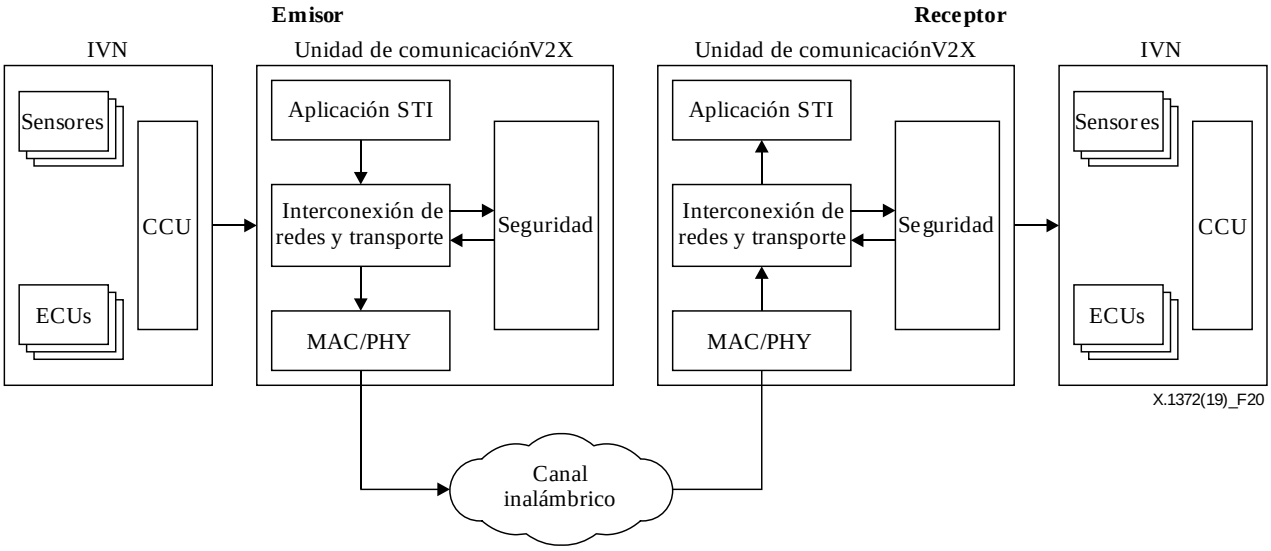


Figura 20 – Procedimiento de alerta de emergencia

9.3 Autentificación de entidades para la comunicación en pelotón

El enfoque en pelotón contempla el modelo de conducción no desde un punto de vista individual, sino grupal. En general, la conducción en pelotón implica la existencia de un grupo de vehículos con intereses comunes donde un vehículo sigue a otro y se mantiene a una distancia corta y casi constante con respecto al vehículo precedente, formando pelotones, como se ve en la Figura 21. En este caso hay tres grandes procesos: integración en el pelotón, cooperación/mantenimiento del pelotón y extracción del pelotón.

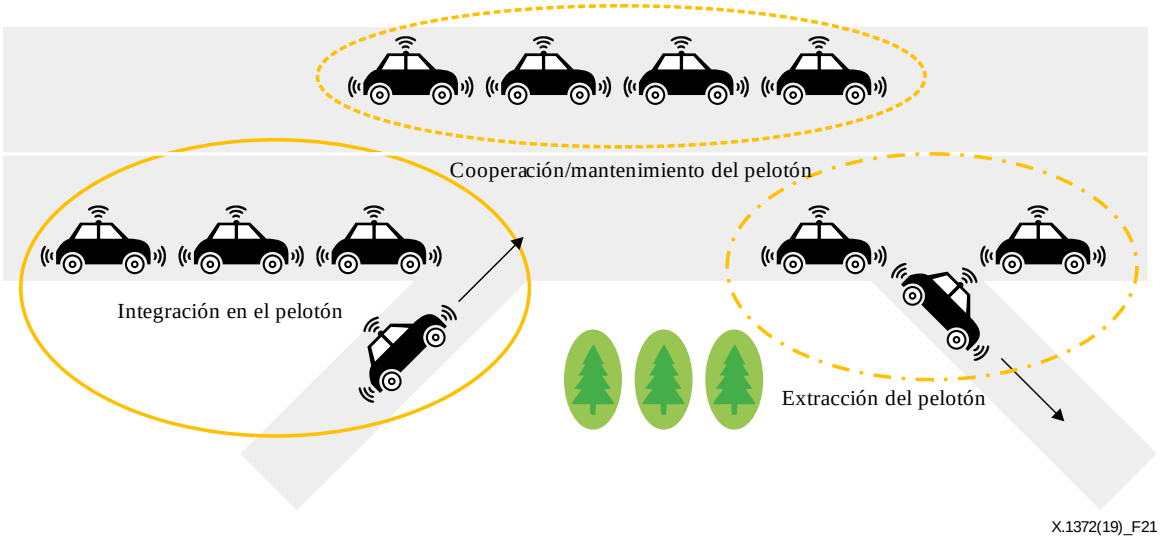


Figura 21 – Caso de uso de la conducción en pelotón

– Formación del pelotón: un vehículo, que no es miembro de un pelotón, se mueve y se integra en el pelotón en el siguiente cruce.

– Cooperación/mantenimiento del pelotón: los vehículos de un mismo pelotón han de comunicar y cooperar unos con otros a fin de mantener el pelotón y ejecutar tareas como dejar paso a vehículos prioritarios, ajustar su posición en función de la ruta planificada, atravesar intersecciones viales y cambiar de carril.

– Extracción del pelotón: el vehículo se extrae del pelotón en la siguiente intersección.

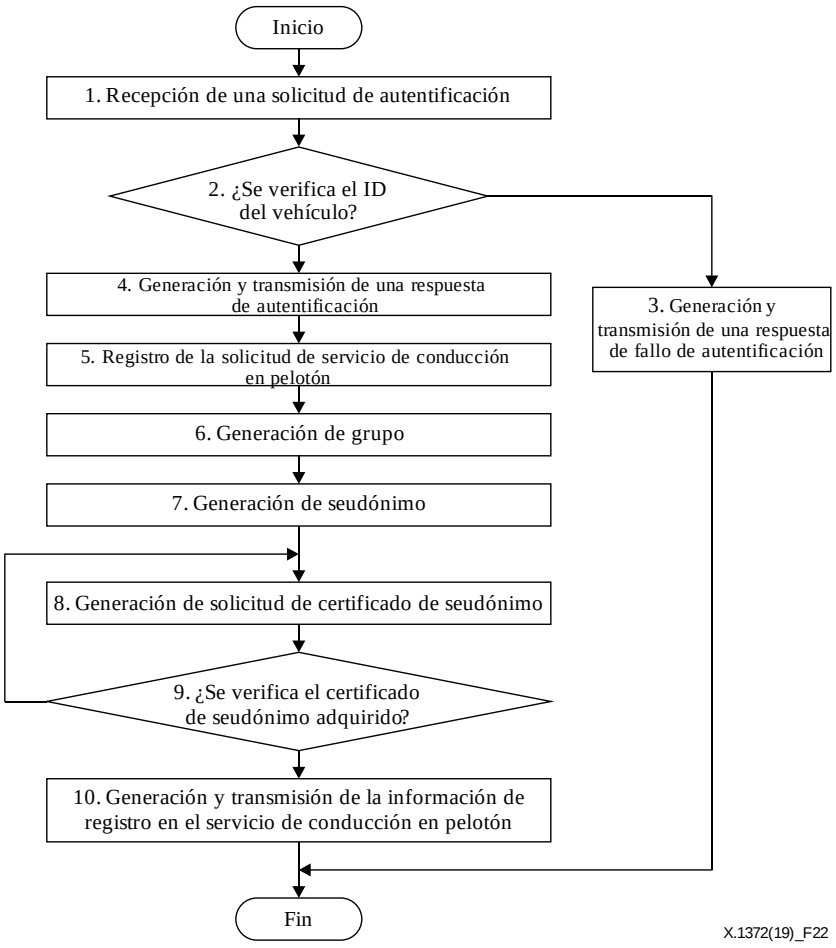


Figura 22–Procedimiento de registro de pelotón

En la Figura 22 se muestra un ejemplo de autentificación para el servicio de conducción en pelotón. Como se ve en la Figura 22, si se recibe de un vehículo una solicitud de autentificación para el registro de un servicio de conducción grupal, es decir, una solicitud de autentificación de vehículo, en modo ejecución de servicio en el paso 1, el ID del vehículo se verificará, por ejemplo, con un algoritmo de firma digital de un sistema criptográfico de clave pública en el paso 2. Por consiguiente, la solicitud de autentificación del vehículo puede presentarse transmitiendo un mensaje firmado con una clave privada del vehículo al sistema de servicio de conducción grupal. Tras la verificación del paso 2, si el ID del vehículo se considera inválido, el sistema del servicio de conducción grupal generará la correspondiente respuesta al fallo de autentificación y la transmitirá a ese vehículo en el paso 3.

Si, tras la verificación del paso 2, se considera que el ID del vehículo es válido, el sistema del servicio de conducción grupal generará una respuesta de autentificación y la transmitirá a ese vehículo en el paso 4.

A continuación, en el paso 5, cuando se recibe la respuesta de autentificación, es decir, cuando se efectúa la autentificación del vehículo después de que el usuario presenta y selecciona la información de registro de conducción grupal, incluida la cualificación de conducción grupal, el punto de partida, el destino, la hora estimada de partida, la hora estimada de llegada y los puntos de descanso deseados, el vehículo transmite la información de registro de conducción grupal al sistema del servicio de conducción grupal a fin de solicitar su registro en el servicio de conducción grupal.

Cuando recibe de un vehículo una solicitud de registro en el servicio de conducción grupal, incluida la información de registro de conducción grupal, el sistema del servicio de conducción grupal genera un grupo a partir de la información de registro de conducción grupal, por ejemplo, idéntico destino, idéntico punto de partida, idéntica hora de llegada estimada, etc., y almacena/registra la información de ese grupo en la información de grupo del paso 6.

El grupo creado debe estar compuesto, como mínimo, de un líder de grupo, es decir, el vehículo líder, y de un miembro, es decir, un vehículo miembro. A partir de ahí, el sistema del servicio de conducción grupal asigna un seudónimo a cada vehículo del grupo en el paso 7, genera un mensaje de solicitud de certificado para que se genere un certificado de seudónimo para los seudónimos asignados a los vehículos del grupo y transmite el mensaje de solicitud de certificado al centro de autentificación en el paso 8.

El sistema del servicio de conducción grupal verifica si se ha obtenido el certificado de seudónimo del centro de autentificación en el paso 9. A continuación, si se verifica el certificado de seudónimo, el sistema del servicio de conducción grupal almacena el certificado de seudónimo en la base de datos de información grupal. El certificado de seudónimo puede ser un mensaje firmado digitalmente del centro de autentificación. Es posible garantizar la justificación del seudónimo con un certificado de seudónimo. El seudónimo es una clave pública signada a cada vehículo por el sistema del servicio de conducción grupal.

Cada vehículo puede recibir varios seudónimos. Dado que el seudónimo carece de información asociada con el ID del vehículo, no queda expuesto el ID de los vehículos que participan en la conducción grupal, por lo que se puede proteger la IIP de cada uno de ellos.

Si se recibe la notificación, en el paso 10 el sistema del servicio de conducción grupal genera la información de registro en el servicio de conducción grupal del grupo creado, almacena esa información en la base de datos de información grupal y la transmite a cada uno de los vehículos del grupo. Esta información de registro en el servicio de conducción grupal puede contener un ID de grupo, el seudónimo asignado a cada vehículo, el certificado de seudónimo para cada uno de ellos, etc. Cada vehículo, es decir, los usuarios de cada vehículo, de un grupo registrado en el servicio de conducción grupal puede proceder y establecer comunicaciones entre los vehículos del grupo utilizando la información de registro en el servicio de conducción grupal que le ha facilitado el mismo servicio.

9.4 Infraestructura de clave pública vehicular

Para inspirar confianza a los participantes en un entorno de comunicación vehicular se necesita una infraestructura de clave pública (PKI, *Public-Key Infrastructure*) que facilite y gestione los certificados digitales. La PKI vehicular difiere de la convencional en varios aspectos, siendo el más importante que los seudónimos se utilizan para proteger la exposición de la localización de un vehículo en relación con la de su propietario. El número de certificados es ingente en comparación con la PKI convencional. Por consiguiente, el principal objetivo de la PKI vehicular es ofrecer métodos eficientes para solicitar certificados y tramitar su revocación.

En el Apéndice II se describen más detalladamente los modelos de referencia de la PKI vehicular.

Apéndice I

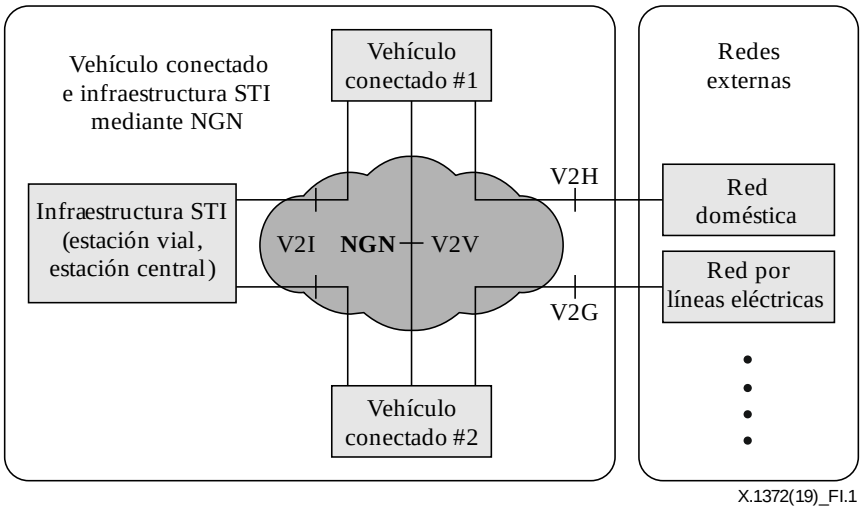
Modelos de referencia para la comunicación vehicular

(Este apéndice no forma parte integrante de la presente Recomendación.)

I.1 Marco de servicios y aplicaciones de vehículos conectados mediante NGN del UIT-T

El marco de servicios y aplicaciones de vehículos conectados en el contexto de las redes de la próxima generación (NGN, *next-generation networks*) se describe en [b-UIT-T Y.2281]. Los vehículos son uno de los componentes clave que utilizan las capacidades de red en las comunicaciones vehículo a infraestructura (V2I), vehículo a vehículo (V2V) y vehículo a domicilio (V2H). En ese contexto, un vehículo conectado puede cooperar con las redes de la próxima generación (NGN) para soportar servicios y aplicaciones más avanzados, como las aplicaciones de seguridad vial, las aplicaciones de tráfico rodado, los servicios multimedia y la implementación de esos servicios en función de la localización.

En [b-UIT-T Y.2281] se identifica la relación entre las NGN y los vehículos conectados y se definen los requisitos aplicables, habida cuenta de la necesidad de soportar servicios y aplicaciones de vehículos conectados utilizando las NGN. Además, se describen un marco arquitectónico de los vehículos conectados por NGN y la infraestructura de los sistemas de transporte inteligentes (STI) a fin de soportar las características de comunicación de las NGN armonizadas con los vehículos conectados.

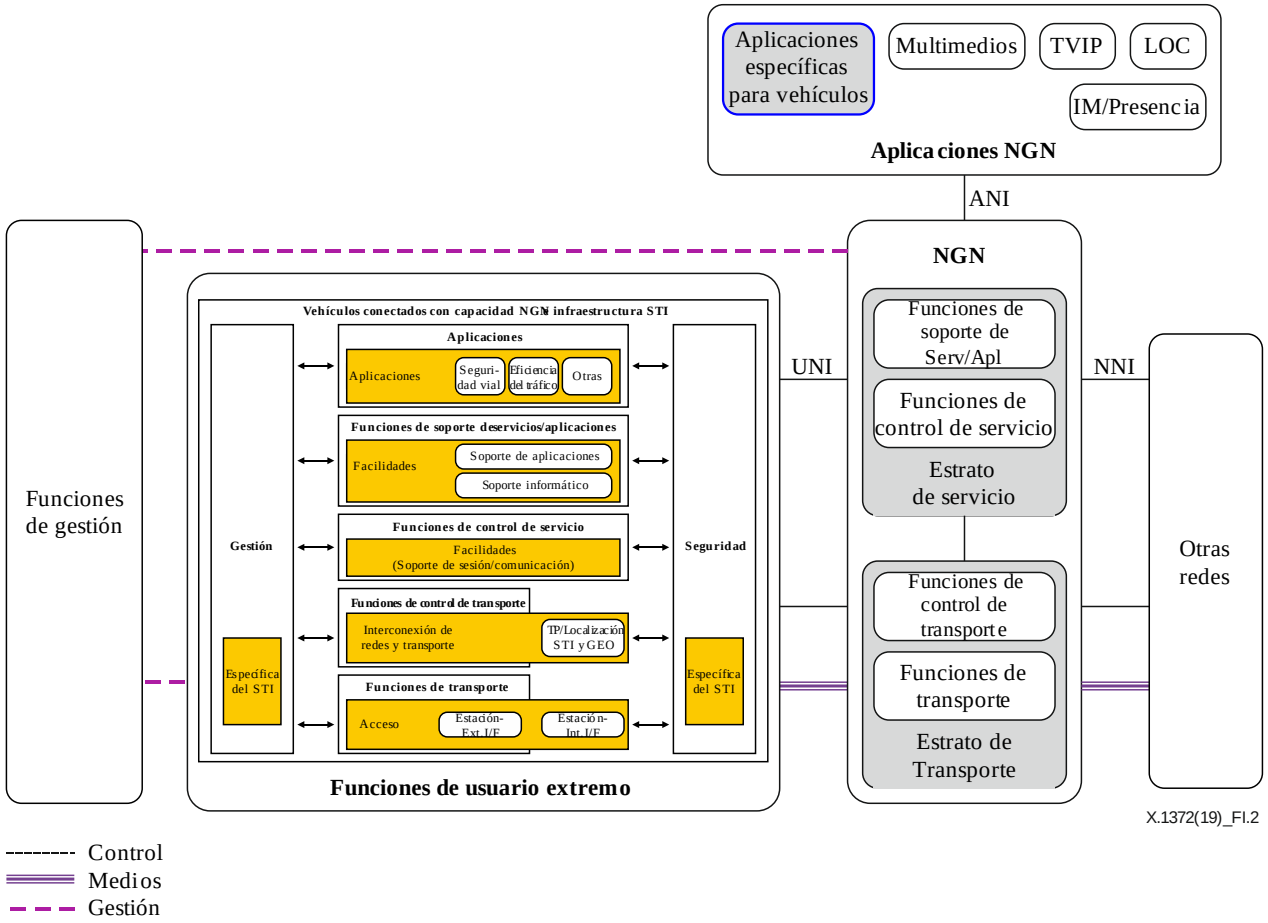


NOTA –Figura retomada de [b-UIT-T Y.2281].

Figura I.1 – Modelos de configuración general de los vehículos conectados y la infraestructura STI

En la Figura I.1 se muestra un modelo de configuración de UIT-T Y.2281 y se ve cómo los vehículos conectados se relacionan con la infraestructura STI y con las redes externas, incluidas las redes domésticas y las redes por líneas eléctricas utilizando las NGN. En comparación con otras normas STI, [b-UIT-T Y.2281] se centra en la utilización de las NGN en el entorno STI. En [b-UIT-T Y.2281] se identifica la utilización de las NGN en los entornos STI para minimizar los problemas de interoperabilidad entre la comunicación STI entre pares y la red pública. Esa interoperabilidad es particularmente importante para la calidad del servicio (QoS), la movilidad y la seguridad de diversos servicios multimedios.

En la Figura I.2 se esboza la arquitectura de los vehículos conectados con capacidad NGN y la infraestructura STI en cooperación con las NGN. Las NGN se componen de "funciones de usuario extremo", un "estrato de servicio", un "estrato de transporte", un "estrato de gestión" y de "aplicaciones NGN". La función de los vehículos conectados con capacidad NGN y la infraestructura STI se encuentra, desde el punto de vista de las NGN, en las funciones de usuario extremo. En [b-UIT-T Y.2281] se describe cómo las aplicaciones NGN propias de los vehículos, como las llamadas de emergencia, se soportan en las NGN.



NOTA – Figura retomada de [b-UIT-T Y.2281].

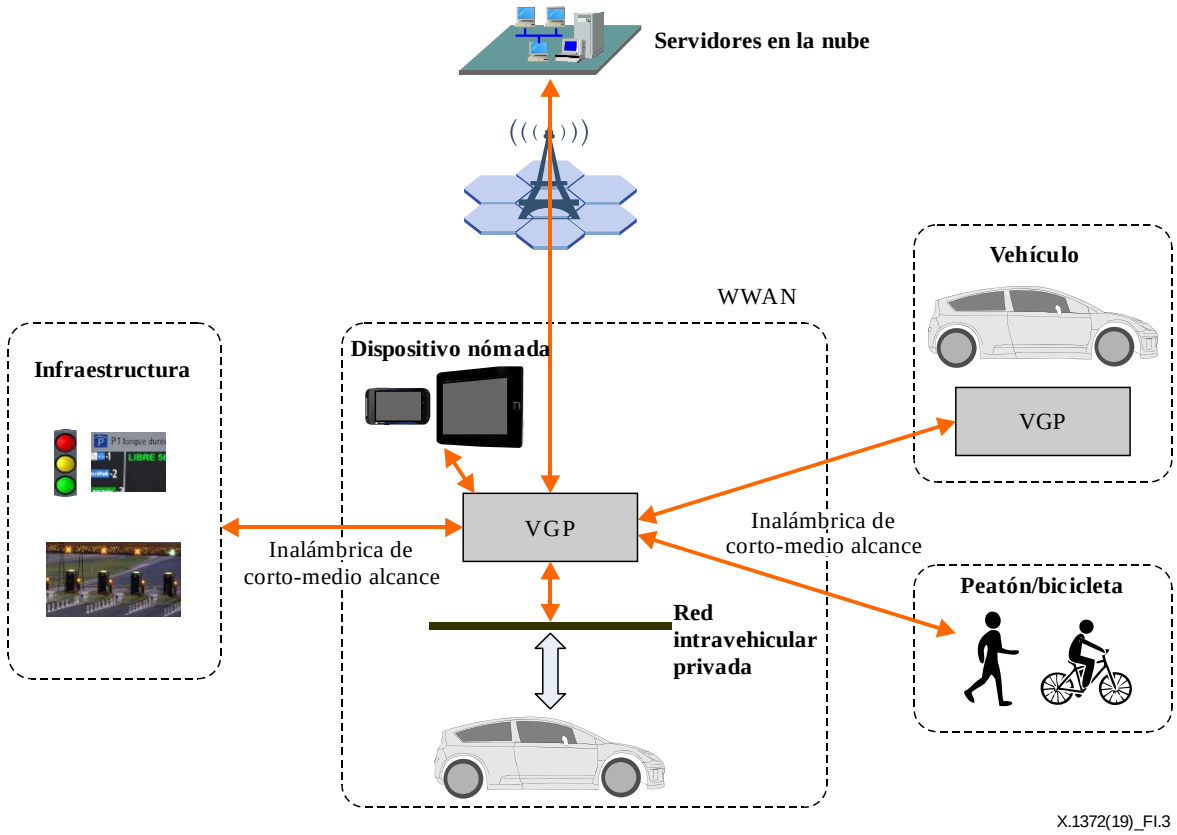
Figura I.2 – Arquitectura de los vehículos conectados con capacidad NGN y la infraestructura STI en cooperación con las NGN

Las consideraciones en materia de seguridad de [b-UIT-T Y.2281] se basan en [b-UIT-T Y.2201]. Las consideraciones en materia de seguridad dependen de la red a la que se conecta el vehículo. Sin embargo, en [b-UIT-T Y.2281] sólo se especifican las consideraciones de seguridad de las NGN y los requisitos de seguridad de otro tipo quedan fuera del alcance de [b-UIT-T Y.2281].

El marco de servicios y aplicaciones de vehículos conectados mediante NGN del UIT-T se centra en la adaptación de las NGN al entorno vehicular. En [b-UIT-T Y.2281] no se especifican los aspectos de seguridad del entorno vehicular. La arquitectura Acceso inalámbrico en el entorno vehicular (WAVE) del IEEE, descrita en [b-IEEE WAVE], se centra en una interfaz radioeléctrica de 5,9 GHz, pues no incluye explícitamente una aplicación para la comunicación con otras redes. La arquitectura STI del ETSI, descrita en [b-ETSI EN 302 665], hace referencia a la capa "aplicación", que es una pila de protocolo para la comunicación. Habida cuenta de que la capa "acceso" comprende IEEE 802.x, 3G celular y Bluetooth, la arquitectura STI del ETSI está prevista para soportar múltiples pilas de protocolo de red.

I.2 Arquitectura y entidades funcionales de las plataformas de pasarela de vehículos del UIT-T

La arquitectura y las entidades funcionales de la plataforma de pasarela de vehículos (VGP, *vehicle gateway platform*) son objeto de estudio de la Comisión de Estudio 16 del UIT-T. La arquitectura, el marco de arquitectura funcional y las entidades funcionales de las plataformas de pasarela de vehículos se describen en [b-UIT-T H.550]. El término VGP se define en [b-UIT-T F.749.1]. Una VGP es el conjunto de hardware y software de TIC de un vehículo que operan como plataforma abierta para crear un entorno de ejecución integrado para la entrega de servicios de comunicaciones de una pasarela de vehículos. Las VGP también pueden ofrecer servicios de comunicaciones de capa superior, como la interacción con el conductor mediante servicios de acceso conductor-vehículo, etc. No se consideran parte de las VGP los subsistemas dedicados exclusivamente al funcionamiento del vehículo.



NOTA – Figura retomada de [b-UIT-T H.550].

Figura I.3 – Situación de la VGP en el modelo de referencia STI

En la Figura I.3 se muestra el posicionamiento de la VGP en el modelo de referencia del sistema de transporte inteligente. Se contemplan seis grandes tipos de comunicación: vehículo a vehículo, vehículo a infraestructura, vehículo a servidor en la nube, vehículo a dispositivo nómada, vehículo a peatón/bicicleta e interacción con la red intravehicular.

– El tipo vehículo a vehículo (V2V) se da cuando los vehículos comunican entre sí con fines de seguridad y de autoconducción.

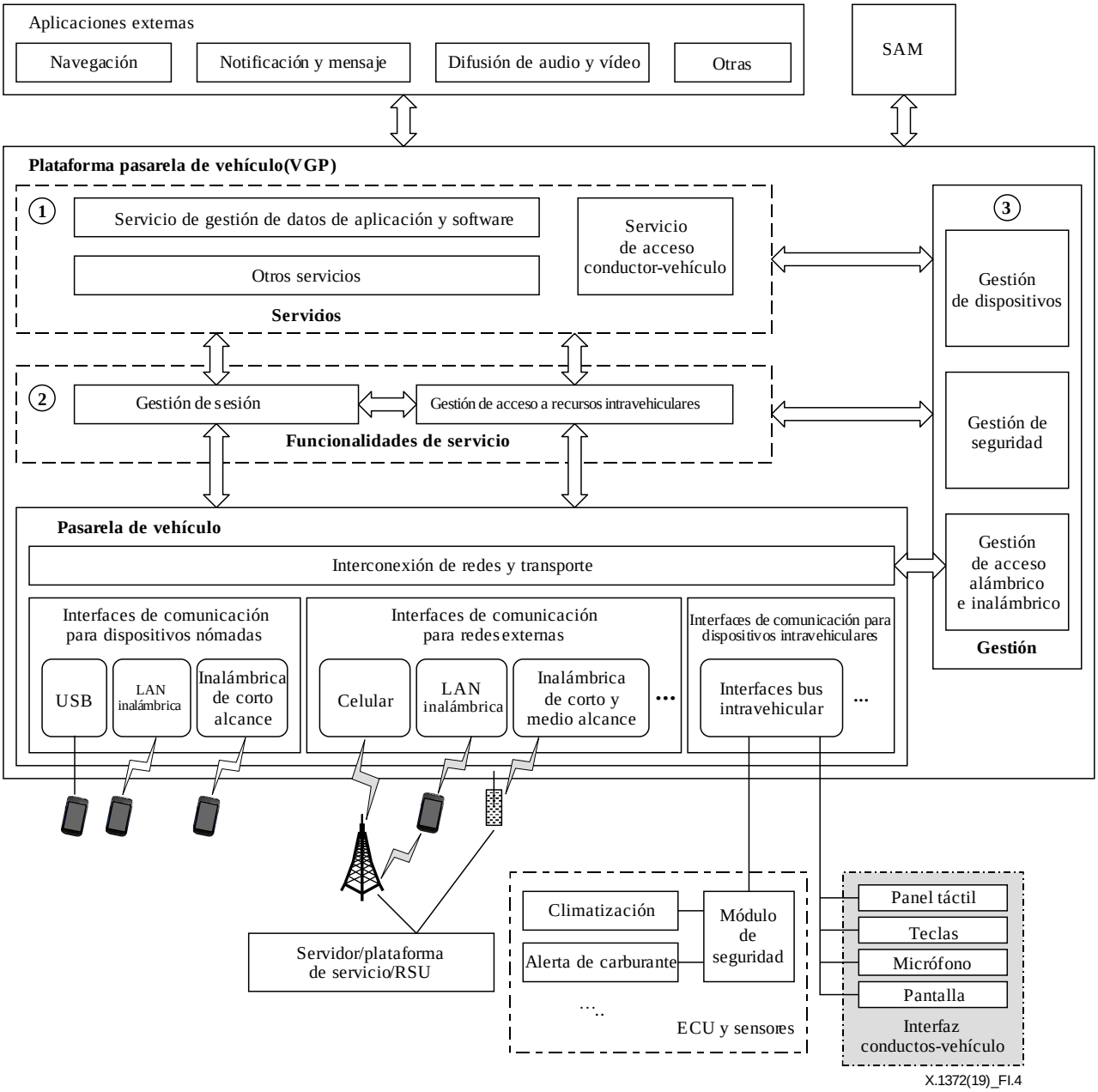
– Por vehículo a infraestructura (V2I) se entiende la comunicación entre vehículos e infraestructuras viales para la seguridad, el cobro electrónico de peajes (ETC, *electronic toll collection*) y el intercambio de información de tráfico.

– La comunicación vehículo a servidor en la nube se da cuando los vehículos comunican con servicios en la nube para llamadas de emergencia y funciones telemáticas.

– El tipo vehículo a dispositivo nómada describe las telecomunicaciones e interfaces de usuario remoto (UI) mediante las cuales los vehículos se conectan a los dispositivos nómadas.

– El caso vehículo a peatón/bicicleta contempla sobre todo las alertas de seguridad cuando los vehículos se comunican con los dispositivos en posesión de los peatones/bicicletas.

– La interacción con la red intravehicular se dedica principalmente al diagnóstico del vehículo, la adquisición de datos a distancia y el control a distancia del vehículo, casos en los que la VGP se comunica con la red intravehicular privada.



NOTA – Figura retomada de [b-UIT-T H.550].

Figura I.4 – Arquitectura de alto nivel de una VGP

En la Figura I.4 se presenta la arquitectura de capa superior de la VGP. Los servicios VGP incluyen el servicio de gestión de datos de aplicaciones y software, el servicio de acceso conductor-vehículo y otros servicios (véase el bloque (1) de la Figura I.4). Entre las funcionalidades de servicio se cuentan la gestión de sesión y la gestión de acceso a recursos intravehiculares (véase el bloque (2) de la Figura I.4). La gestión comprende la gestión de dispositivos, la gestión de seguridad y la gestión de acceso alámbrico e inalámbrico (véase el bloque (3) de la Figura I.4). Los servicios dan soporte a aplicaciones externas, como la navegación y el infoocio en forma de establecimiento de sesión, conversión del formato de datos y procesamientos específicos.

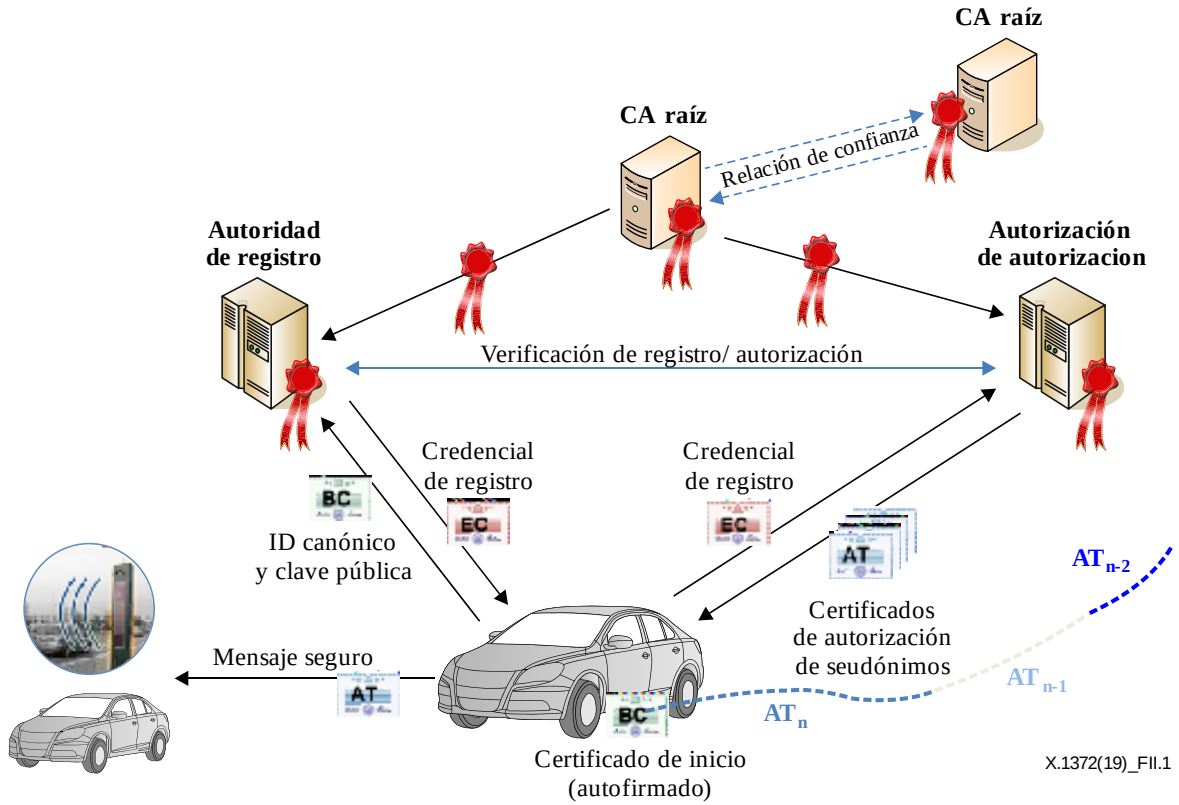
Los aspectos de seguridad de la VGP forman parte de la capa de gestión descrita en [b-UIT-T H.550], en cuya cláusula 8.4.1 de [b-UIT-T H.550], "Gestión de seguridad", puede encontrarse una descripción genérica de la función de seguridad, que consiste en la gestión de seguridad para la capa de acceso, que comprende las capas de transporte y red, y la gestión de seguridad para servicios/aplicaciones.

Apéndice II

Modelos de referencia de PKI vehicular

(Este apéndice no forma parte integrante de la presente Recomendación.)

En la actualidad las funcionalidades de seguridad de la comunicación STI comprenden la autentificación de mensajes, que influye en la privacidad de vehículos y conductores. A nivel europeo, el Instituto Europeo de Normas de Telecomunicaciones (ETSI) ha definido un mecanismo de autentificación de mensajes basado en la utilización de una infraestructura de clave pública (PKI), como la PKI vehicular que se ilustra en la Figura II.1.



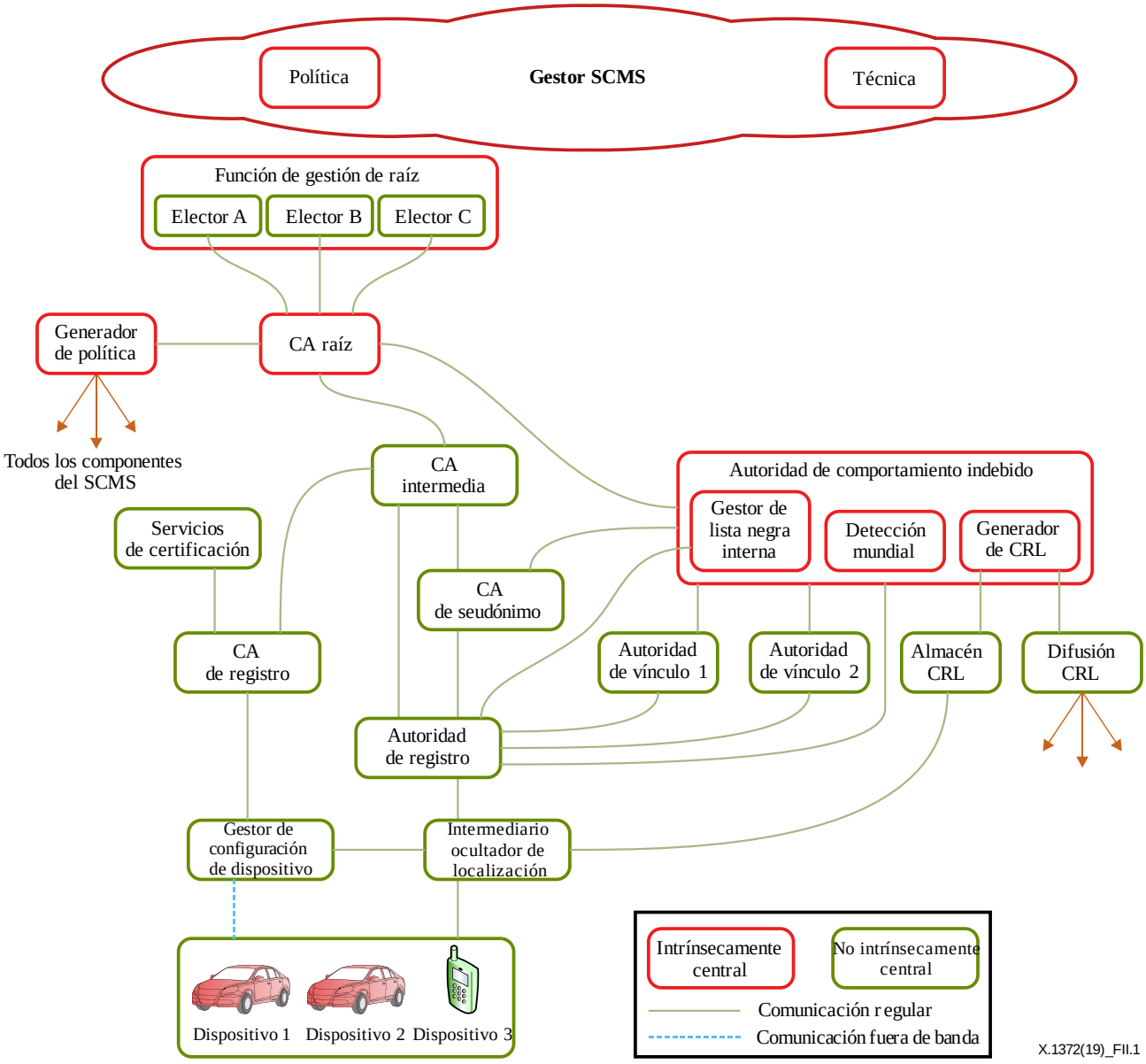
NOTA – Fuente [b-ETSI TS 102 940].

Figura II.1 – PKI vehicular del ETSI

La autoridad de certificación raíz (RCA, *root certificate authority*) es el punto de partida de la cadena de confianza de certificación: firma los certificados de otras autoridades (autoridad de autorización (AA, *authorization authority*) y autoridad de registro (EA, *enrolment authority*)) y crea y mantiene la lista de revocación de certificados, (CRL, *certificate revocation list*) y la lista de autoridades revocadas. En el contexto operativo, la RCA está gestionada por una entidad que puede garantizar un nivel de confianza elevado y estable y que es suficientemente federativa, como un Estado o un grupo de Estados. La EA es la autoridad que expide los certificados de registro (EC, *enrolment certificates*) y valida las solicitudes de tique de autorización (AT, *authorization tickets*). La AA es un tercero fiable que entrega AT a las estaciones STI. La AA desconoce la identidad de la estación STI y confía en que la EA verifique si la estación STI está o no autorizada a poseer un AT. La solicitud de AT contiene la identidad de la EA ante la cual está registrada la estación STI.

Esta arquitectura está destinada a ofrecer privacidad a las estaciones STI y evitar su rastreo: la EA conoce la identidad de la estación STI, pero desconoce el certificado de seudónimo (AT) que utiliza, mientras que la AA conoce el certificado de seudónimo de la estación STI, pero desconoce su identidad. Una estación STI se registra ante la EA y obtiene un certificado de registro. El EC se utiliza para solicitar un seudónimo (AT) a la AA. Cuando una estación STI solicita un AT, envía en el mensaje de petición su identidad encriptada con el EC y la identidad de la EA. La AA recibe la solicitud de seudónimo, lee el identificador de la EA y verifica el punto de acceso de la EA para validar la solicitud de AT. La EA verifica el EC de la estación STI y valida (o no) la solicitud. Si se valida la solicitud, la AA genera y envía el AT a la estación STI.

Por otra parte, la CAMP (*crash avoidance metrics partnership*) presentó un sistema de gestión de credenciales de seguridad (SCMS, *security credential management system*) para asegurar las comunicaciones V2X (véase [b-SCMS]). Este sistema se basa en la PKI para la seguridad V2X y en la actualidad está en fase de transición entre la investigación y el prototipo. El SCMS soporta la inicialización, la configuración de certificados, la comunicación de comportamientos indebidos y la revocación.



NOTA – Fuente [b-SCMS].

Figura II.2 –Arquitectura V-PKI de CAMP

En la Figura II.2 se ilustra la arquitectura del SCMS. Las líneas definen las relaciones entre los distintos componentes del SCMS y se indica cada componente que envía información o certificados a otros.

Los principales componentes del SCMS son los siguientes:

– CA de registro (ECA): expide certificados de registro para los dispositivos y puede utilizarse para solicitar certificados de seudónimo para distintas regiones geográficas, fábricas o tipos de dispositivos.

– CA intermedia (ICA): es una autoridad de certificación secundaria que impide la sobrecarga de la CA raíz. Su certificado está expedido por la CA raíz.

– Autoridad de vínculo (LA): genera valores previnculo para formar los valores de vínculo de los certificados para su eficiente revocación. Además, se prevé que haya varias LA para evitar que el operador de una LA vincule los certificados de un dispositivo concreto.

– Intermediario de ocultación de localización (LOP): cambia la dirección de origen para ocultar la localización del dispositivo solicitante y evitar la vinculación de las direcciones de red con localizaciones.

– Autoridad de comportamiento indebido (MA): recibe y procesa los informes de comportamiento indebido de los dispositivos para identificar los posibles comportamientos indebidos o fallos de funcionamiento. Además, revocará el certificado del dispositivo y lo incluirá en la CRL. La MA también inicia el proceso de vinculación de un identificador de certificado con los certificados de registro correspondientes y lo pondrá en la lista negra interna de la RA.

– Generador de política (PG): se ocupa de la actualización del fichero de política global de la RA. El fichero de política global contiene la información de configuración global y el fichero de cadena de certificados global, que integra todas las cadenas de confianza del SCMS.

– CA de seudónimo (PCA): expide los seudónimos a corto plazo, las identificaciones y los certificados de aplicación para los certificados. Cada PCA se limita a una zona geográfica concreta, un fabricante concreto o un tipo de dispositivo específico.

– Autoridad de registro (RA): valida y procesa las solicitudes de los dispositivos y garantiza que los dispositivos revocados no puedan obtener nuevos certificados de seudónimo. Además, la RA no expide más de un juego de certificados con una validez determinada para cada dispositivo. Por otra parte, la RA mezclará las solicitudes o informes antes de enviar las solicitudes de firma de certificados de seudónimo a las PCA o de remitir la información a la MA.

– Autoridad de certificación raíz (RCA): es la raíz y entidad principal de la cadena de certificación del SCMS. Expide los certificados para las ICA, los PG y las MA.

Bibliografía

[b-UIT-T F.749.1] Recomendación ITU-T F.749.1 (2015), *Requisitos funcionales de las pasarelas de vehículos*.

[b-UIT-T H.550] Recomendación UIT-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms.*

[b-UIT-T X.509] Recomendación UIT-T X.509 (2019), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

[b-UIT-T X.641] Recomendación UIT-T X.641 (1997), T*ecnología de la información – Calidad de servicio: marco.*

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), A*rquitectura de seguridad de la interconexión de Sistemas Abiertos para aplicaciones del CCITT*.

[b-UIT-T X.813] Recomendación UIT-T X.813 (1996), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo.*

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones de referencia para la gestión de la identidad.*

[b-UIT-T X.1371] Recomendación UIT-T X.1371 (2019), *Amenazas a la seguridad de los vehículos conectados*.

[b-UIT-T Y.2201] Recomendación UIT-T Y.2201 (2009), *Requisitos y capacidades de las redes de próxima generación del UIT-T.*

[b-UIT-T Y.2281] Recomendación UIT-T Y.2281 (2011), *Marco para servicios y aplicaciones de vehículos interconectados mediante el uso de NGN*.

[b-ETSI EN 302 665] ETSI EN 302 665 V1.1.1 (2010-09), *Intelligent Transport Systems(ITS); Communications Architecture*.
<https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf>

[b-ETSI TS 102 940] ETSI TS 102 940 V1.3.1 (2018-04), *Intelligent Transport Systems(ITS); Security; ITS communications security architecture and security management.*
<https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf>

[b-IEEE WAVE] IEEE Std. 1609.2 (2016), *IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages.*

[b-ISO 13185-1] ISO/TR 13185-1:2012, *Intelligent transport systems – Vehicle interface for provisioning and support of ITS services – Part 1: General information and use case definition.*

[b-OVERSEE] Open Vehicular Secure Platform, OVERSEE Project. (Website).
<https://www.oversee-project.com/>

[b-RITA] United States Department of Transportation, FHWA-JPO-11-130 (2011), *An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues*.
<https://rosap.ntl.bts.gov/view/dot/3334/Share>

[b-SCMS] Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium, *Security Credential Management System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.1, 04*. May. 2016. <https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf>

[b-UNECE GRVA] United Nations Secretary of the Informal document GRVA-01-17, *Draft recommendation on cyber security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA.*

[b-US DOT] United States Department of Transportation, Safety Pilot Program. <https://www.its.dot.gov/research_archives/safety/safety_pilot_plan.htm>

[b-USDOTHS812014] United States Department of Transportation, National Highway Traffic Safety Administration, DOT HS 812 014 (2014), *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application.* <https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>

[b-US GOV] United States Senator for Massachusetts, Edward J, Markey, Staff Report (2015), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk.* <http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2020

Impreso en Suiza
Ginebra,