Diseño de un protocolo para el envío de notificaciones de denuncias por hechos de circulación al vehículo a través de tecnologías ITS

José María de Fuentes García-Romero de Tejada
Ingeniero en Informática. Profesor Ayudante. Universidad Carlos III de Madrid[1]

Ana Isabel González-Tablas Ferreres
Doctora en Ingeniería Informática. Profesora Titular. Universidad Carlos III de Madrid

Lorena González Manzano
Ingeniera en Informática. Personal Investigador en Formación. Universidad Carlos III de Madrid

Arturo Ribagorda Garnacho
Doctor en Informática. Catedrático. Universidad Carlos III de Madrid

RESUMEN: Los mecanismos actualmente existentes para la notificación consiguen que ésta llegue a su destinatario varios días después a la comisión del hecho. Esta circunstancia juega en contra del potencial educativo de la sanción, el cual crece con la inmediatez.
El marco tecnológico que plantean los ITS permite atisbar un nuevo canal de notificación, directo al vehículo. De esta forma, el conductor podría recibir dicho mensaje con máxima rapidez, posibilitando un potencial cambio en su conducta.
En este trabajo se propone el diseño de un protocolo de intercambio de datos entre un vehículo y la infraestructura de comunicaciones ITS. Además, se analiza el cumplimiento de los requisitos legales por parte del protocolo, así como sus costes computacionales y de red considerando una plataforma ITS comercial. En este último aspecto es imprescindible tener en cuenta los costes de la aplicación de técnicas criptográficas que serán necesarias para garantizar la integridad, confidencialidad y autenticidad de los datos en juego.

1 INTRODUCCIÓN

[1] Universidad Carlos III de Madrid. Avenida de la Universidad, 30, 28911 Leganés (Madrid)
Teléfono de contacto: 0034 91 624 5957
Correo electrónico: {jfuentes, aigonzal, lgmanzan, arturo } @ inf.uc3m.es

La gran cantidad de accidentes y víctimas de tráfico urge a la búsqueda de nuevas soluciones que permitan evitar, en lo posible, la ocurrencia de incidentes de tráfico. Uno de los mecanismos para reducir la siniestralidad reside en promover el cumplimiento de las normas de tráfico. Con la intención de corregir aquellos comportamientos que vayan en contra de las normas, existe un mecanismo de sanciones que se aplican sobre el infractor. Para garantizar que toda infracción es adecuadamente sancionada, se ha diseñado un procedimiento sancionador.

En el caso concreto de España, el procedimiento sancionador arrastraba una serie de problemas que ponían en riesgo su eficacia. Entre ellos, el sistema de notificaciones basado en el correo postal introducía retrasos y, si los datos no estaban convenientemente actualizados, originaba que la notificación no llegara al infractor. A tenor de este hecho, la Ley 18/2009 reformó dicho procedimiento para agilizar la tramitación de las sanciones [2]. En lo que afecta a las notificaciones, dicha Ley introducía la posibilidad de realizar el envío por medios telemáticos. Con este fin, la Ley 11/2007 [5] y el Real Decreto 1671/2009 [3] que la desarrolla parcialmente contemplan cuatro posibles mecanismos: una dirección electrónica habilitada (que, en el ámbito del tráfico, se conoce como Dirección Electrónica Vial (DEV) [2]), una dirección de correo electrónico con acuse de recibo, la comparecencia electrónica y cualquier otro “siempre que quede constancia de la recepción por el interesado en el plazo y en las condiciones que se establezcan en su regulación específica”[3].

Uno de los elementos en los que incide la Ley es en garantizar que el infractor tenga garantizado su “derecho a conocer” los procedimientos en los que está implicado. Sin embargo, los tres primeros mecanismos citados anteriormente sólo permiten que el conductor tenga conocimiento de la infracción, como pronto, una vez finalizado el viaje. Esta circunstancia, además, disminuye la capacidad educativa de la sanción al producirse ésta en un momento muy posterior al hecho que la origina [4]. Esta necesidad de inmediatez, junto con la exigencia de que el conductor disponga de un “lugar cierto de notificaciones donde todas las Administraciones de tráfico puedan remitirle las diferentes comunicaciones” [2], motivan la búsqueda de un nuevo mecanismo de notificación. Dicho mecanismo puede utilizar tecnologías que no estén explícitamente contempladas en la legislación, pues tal y como expone la Ley 11/2007, “la Ley no puede limitarse a regular el uso de los canales electrónicos disponibles hoy en día” [5].

Las tecnologías ITS permiten la distribución de información de forma directa a los vehículos. En este sentido, el proceso de notificación podría realizarse a través de un mecanismo

basado en tecnologías ITS. Así, el vehículo podría recibir el mensaje de notificación y, empleando su interfaz de comunicación con el conductor, transmitirle dicho mensaje de forma tal que no supusiera una distracción. No obstante, es preciso diseñar el mecanismo de notificación garantizando que, por un lado, se satisfacen los requisitos legales que determinan la validez de la notificación y, por otro, es posible su realización teniendo en cuenta las limitaciones técnicas (e.g. recursos computacionales y de red) que imponen las tecnologías ITS actuales.

En este trabajo se describe un mecanismo para el envío de la notificación de tráfico al vehículo utilizando tecnologías ITS. Dicho mecanismo es analizado tanto desde el punto de vista del cumplimiento de las restricciones legales como del rendimiento técnico ofrecido.

Organización del artículo. La Sección 2 introduce los aspectos básicos de los sistemas ITS y de la notificación. La Sección 3 presenta el protocolo propuesto, describiendo el modelo, la arquitectura y el mecanismo de intercambio de mensajes. La Sección 4 analiza el protocolo propuesto considerando las cuestiones técnico-legales. La Sección 5 describe los trabajos relacionados. La Sección 6 presenta las conclusiones del trabajo y las líneas futuras.

2 CONCEPTOS PREVIOS

En esta Sección se introducen los conceptos previos imprescindibles para comprender la propuesta. Particularmente, la Sección 2.1 introduce los sistemas inteligentes de transporte y sus tecnologías relacionadas, la Sección 2.2 describe brevemente los servicios básicos de seguridad de la información y sus mecanismos asociados. Las restantes secciones abordan la notificación electrónica, presentando sus mecanismos actuales (Sección 2.3), su modelo subyacente (Sección 2.4) y el contenido de una notificación (Sección 2.5).

2.1 Sistemas Inteligentes de Transporte. Tecnologías relacionadas

Los Sistemas Inteligentes de Transporte (conocidos comúnmente como ITS por sus siglas en inglés) proceden de la aplicación de las tecnologías de la información y las comunicaciones sobre los vehículos. Así, los vehículos pueden comunicarse no sólo entre sí, sino también con uno o varios proveedores de servicios ITS. Dichos servicios pueden relacionarse con la mejora de la seguridad vial, la asistencia al conductor o la mejora de la comodidad de los pasajeros. En cualquier caso, el servicio se presta mediante el

intercambio de información del vehículo con otros colindantes o con los proveedores de servicios.

2.1.1 Dispositivos y tecnologías de comunicación

Para que la comunicación desde y hacia el vehículo sea posible, éstos deben equiparse con un dispositivo de comunicaciones conocido como On-Board Unit (OBU), que permite la utilización de diversas tecnologías de comunicación, siendo las más comunes la tecnología celular y la tecnología DSRC. Si bien la primera es común para otros dispositivos actuales (e.g. telefonía móvil), DSRC es una tecnología específicamente diseñada para el ámbito vehicular y particularmente adaptada a la gran velocidad a la que se mueven los vehículos. La comunicación DSRC es de corto alcance, por lo que para lograr la conectividad de los vehículos con los proveedores de servicios es necesario disponer de una infraestructura en el lateral de la carretera compuesta por antenas (conocidas como RSU, del inglés Road-Side Unit).

2.1.2 Plataforma intra-vehicular de computación

Además de la mencionada OBU, existen numerosos dispositivos en el interior del vehículo relacionados con los ITS. A fin de garantizar la confiabilidad del funcionamiento de dichos dispositivos en conjunto, el proyecto OVERSEE[2] propone una arquitectura funcional de los mismos (Figura 1). En ella, existe un dispositivo de seguridad hardware que ejerce de raíz de confianza, gracias al cual la integridad y buen funcionamiento de los demás dispositivos queda asegurada. Dicho dispositivo dispone de capacidad para realizar operaciones criptográficas y de un almacenamiento confiable. Así mismo, proporciona una fuente de tiempo fiable [6].

El funcionamiento de la arquitectura se basa en el dispositivo de seguridad mencionado. Así, una vez que el dispositivo se inicializa, se encarga de iniciar los elementos principales de la arquitectura: una red de interconexión, un controlador software criptográfico, una partición segura de entrada y salida y la partición donde residen las aplicaciones ITS a ejecutar desde el vehículo. La partición de entrada-salida está conectada, a su vez, a la interfaz de interacción hombre-máquina y a la Unidad de Comunicaciones OBU.

[2] https://www.oversee-project.com/

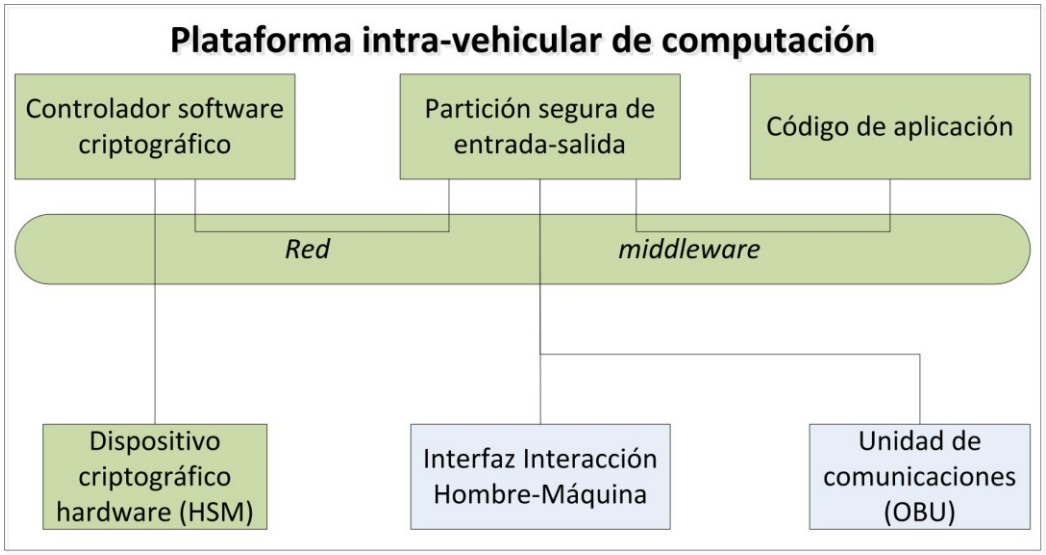

Figura 1. Plataforma intra-vehicular propuesta por OVERSEE

El alcance de la comprobación del buen funcionamiento no alcanza a todos los elementos de la arquitectura. En particular, tanto la interfaz de interacción hombre-máquina como la OBU quedan fuera de dicho alcance. Por este motivo, ambos componentes pueden ser comprometidos. Si bien el compromiso de la interfaz no parece tener un beneficio asociado, la OBU permitiría controlar su funcionamiento a voluntad del atacante. Esto le permitiría desviarse de los protocolos establecidos para el normal uso de las aplicaciones y servicios ITS, tratando potencialmente de obtener un mayor beneficio. A modo de ejemplo, esto permitiría que la OBU no participara en tareas de encaminamiento de mensajes, que resultan imprescindibles para el sostenimiento de la red vehicular basada en la tecnología DSRC introducida anteriormente.

2.2 Servicios de seguridad y mecanismos criptográficos asociados

De acuerdo a la ISO 7498-2 existen cinco servicios de seguridad [18]: *integridad*, que garantiza que el mensaje no ha sido modificado desde su creación; *confidencialidad*, que garantiza que terceros no autorizados no pueden acceder al mensaje; *no repudio* (sobre una acción), que impide que una entidad niegue haber realizado dicha acción; *autenticación*, que garantiza que una entidad es quien dice ser; y *control de acceso*, que determina qué acciones puede llevar a cabo una entidad debidamente autenticada. Además de esto, se suele considerar la *disponibilidad*, que garantiza que una entidad o servicio está disponible para su uso.

Para proporcionar los anteriores servicios, a excepción de la disponibilidad (cuya provisión se asegura mediante un dimensionamiento adecuado del elemento en cuestión), y del control de acceso (que se puede gestionar a través de políticas), los demás servicios disponen de uno o más servicios criptográficos que los proporcionan. La Tabla 1 muestra la relación entre servicios y mecanismos, y especifica las implementaciones concretas de éstos que se utilizan en el entorno vehicular de acuerdo al estándar IEEE 1609.2 [7]. Así mismo, presenta la notación que se emplea para referirlas, siendo *m* el mensaje sobre el que se aplica el mecanismo en cuestión. Es preciso destacar que para los mecanismos de cifrado y firma electrónica escogidos en el ámbito vehicular, es necesario hacer uso de criptografía de clave pública. En ella, existe un par de claves (una privada y una pública), asociadas criptográficamente, de forma que las acciones realizadas con una pueden ser invertidas con la otra. Así, el cifrado se realiza con la clave pública del destinatario, y el descifrado con la privada. Con respecto a la firma, se realiza con la clave privada del firmante y se verifica con su pública. La esencia de este tipo de criptografía radica en que la clave privada se mantiene bajo la custodia exclusiva de la entidad con la que se relaciona. La asociación entre una entidad y su par de claves queda acreditada mediante un documento electrónico, denominado certificado de clave pública, que es emitido por una entidad conocida como *autoridad de certificación*.

Tabla 1. Relación entre servicios de seguridad, mecanismos que los proporcionan en el ámbito vehicular y notación

Mecanismo	**Servicio**	**Implementaciones seleccionadas en el ámbito vehicular [7]**	**Notación**
Firma electrónica	Integridad, no repudio (en emisión), autenticación (origen del mensaje)	ECDSA (en este trabajo, se escoge la variante ecdsa_nistp224_with_sha224)	$S_{Entidad}(m)$
Función resumen	Integridad	SHA-256	H(m)
Cifrado	Confidencialidad	ECIES	$E_{Entidad}(m)$

2.3 Mecanismos de notificación electrónica

El proceso de notificación es el mecanismo por el cual se envía al infractor un mensaje de forma que surte los efectos oportunos en el procedimiento. Así, la notificación debería ser un proceso ágil. Por ello, la Ley 30/92 permite el uso de nuevos mecanismos "distintos a los tradicionales que, sin merma de las necesarias garantías de autenticidad, permitan su agilización mediante el empleo de las nuevas técnicas de transmisión de información, superándose la limitación de la exclusividad del domicilio como lugar de notificaciones" [8]. En particular, el uso de medios telemáticos queda contemplado en la misma Ley (tras su reforma por la Ley 24/2001), exigiendo previamente que "el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización".

Con respecto a las consideraciones necesarias para realizar la notificación, la misma Ley establece que es necesario "tener constancia de la recepción por el interesado o su representante, así como de la fecha, la identidad y el contenido del acto notificado" [8].

En base a la experiencia de la citada Ley, la Ley 11/2007 y, particularmente, el Real Decreto 1671/2009 que la desarrolla parcialmente, establece cuatro mecanismos para la notificación electrónica: uso de una dirección electrónica habilitada, el uso de una dirección de correo electrónico con acuse de recibo, la comparecencia electrónica y cualquier otro que pueda establecerse "siempre que quede constancia de la recepción por el interesado en el plazo y en las condiciones que se establezcan en su regulación específica" [3].

Si bien el mecanismo propuesto en este trabajo se encuadra bajo el último de los supuestos, parece necesario analizar los requisitos exigidos a los demás mecanismos de notificación para adelantarse a esa "regulación específica" que, en lo posible, debería otorgar las mismas garantías a los ciudadanos. Así, para la dirección electrónica habilitada se exige que se acredite la fecha y hora de la puesta a disposición, así como la de acceso a su contenido. Se exige también que se posibilite un acceso permanente y un mecanismo de autenticación que garantice la exclusividad de su uso y la identidad del usuario. Además, la Orden PRE-878/2010 establece una serie de requisitos adicionales para aquellos organismos que no dispongan de su mecanismo específico. Dichos requisitos exigen preservar la confidencialidad de la información transmitida y la disponibilidad del servicio, el uso de medidas de seguridad física, protección de los soportes, control de los accesos y la acreditación temporal utilizando el Real Observatorio de la Armada [9].

En el caso de la dirección de correo electrónico, se exige que se genere un acuse de recibo, de forma inevitable y automática, en el momento de acceso al contenido. Finalmente, en la comparecencia electrónica, el usuario debe estar debidamente identificado y visualizar, en primer lugar, una advertencia sobre el carácter de notificación del mensaje. Aceptada esta condición, el sistema deberá registrar la fecha y la hora de acceso al contenido [3].

2.3.1 Mecanismo específico del procedimiento sancionador de Tráfico: Dirección Electrónica Vial (DEV)

En el ámbito del procedimiento sancionador de Tráfico, la Ley 18/2009 apuesta por la utilización de un tipo específico de dirección electrónica habilitada conocida como Dirección Electrónica Vial (DEV). Gracias a la DEV, "el tradicional concepto de domicilio físico se transforma ahora en domicilio virtual" [2]. Dicho mecanismo pretende ofrecer "garantía material" de que el ciudadano "tenga siempre conocimiento de los procedimientos que contra él se dirigen".

Ante una notificación recibida, el destinatario puede aceptarla o rechazarla. Para evitar la prolongación en el tiempo ante la toma de esta decisión, una vez transcurridos "diez días naturales sin que se acceda a su contenido, se entenderá que aquélla ha sido rechazada, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso" [2].

Los requisitos que dicha Ley impone sobre la DEV son muy similares a los que se le imponen a la dirección electrónica habilitada. Así, se deberá "acreditar la fecha y hora en que se produzca la puesta a disposición del denunciado del acto objeto de notificación, así como el acceso a su contenido" [2]. Se omiten así las consideraciones sobre el acceso permanente y la necesidad de autenticación, aunque parece lógico pensar que éstas se presuponen.

2.4 Modelo subyacente

A excepción del último mecanismo propuesto en el R.D. 1671/2009 (que está sujeto a su regulación específica), los tres primeros se rigen por un modelo equivalente, presentado en la Figura 2. La Dirección Electrónica Vial, en tanto que dirección electrónica habilitada, queda también descrita bajo el mismo modelo.

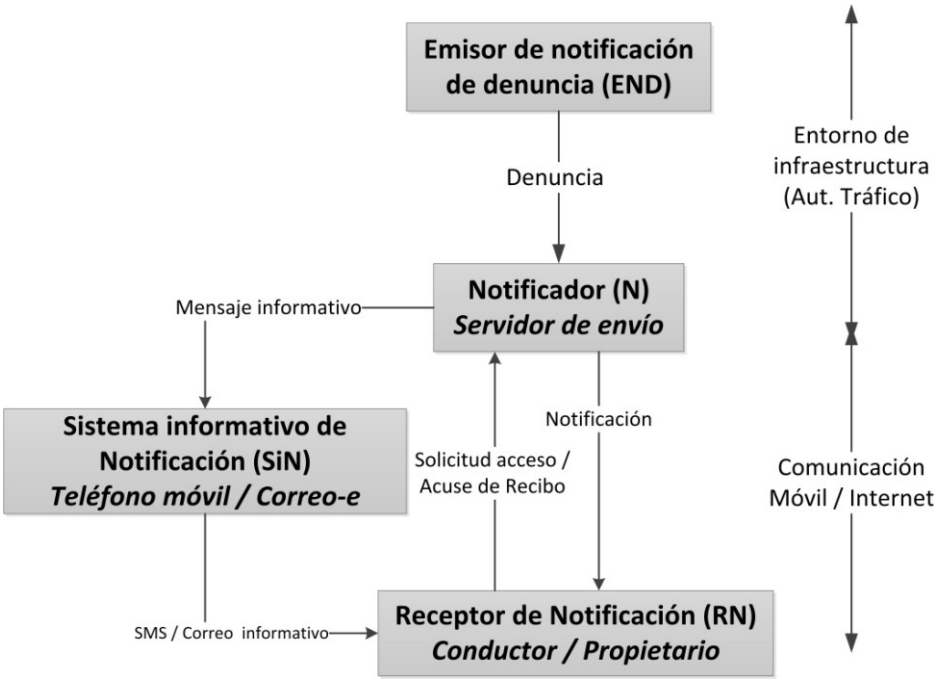

Figura 2. Modelo de los mecanismos de notificación electrónica regulados por el R.D. 1671/2009

Una vez que el mensaje es creado por el Emisor de Notificación de Denuncia (END), se pone a disposición del interesado a través de un Notificador (N), el cual se encarga no sólo de distribuir el mensaje al Receptor de la Notificación (RN) sino también de enviar un mensaje informativo sobre la existencia de la denuncia. Dicho mensaje informativo se hace llegar a RN a través del Sistema informativo de Notificación (SiN).

La relación entre estas entidades se produce en dos entornos distintos de comunicación. Si bien la conexión entre END y N tiene lugar en el entorno de la infraestructura de la Autoridad de Tráfico, la relación entre N, SiN y NR se realiza en el ámbito de las comunicaciones móviles e Internet.

2.4.1 Modelos de interacción

Con vistas a permitir el acceso a la notificación por parte del RN, se produce un intercambio de solicitud-respuesta entre éste y el Notificador.

A la vista de los mecanismos previstos en la actual legislación, existen dos modelos para realizar dicho intercambio: *push* (en el que el Notificador envía la notificación y, posteriormente, RN envía un acuse de recibo, a modo de acreditación de acceso) y *pull* (en el que RN previamente solicita el acceso a la notificación). El modelo push es el seguido por

la dirección de correo electrónico, mientras que la dirección electrónica habilitada y la comparecencia electrónica siguen el modelo pull.

2.5 Contenido de la notificación

De acuerdo a la Ley 18/2009, las notificaciones[3] deben contener los siguientes elementos:

a) **Sobre el infractor:** la identificación del vehículo, la del denunciado (si fuera conocida). El domicilio que, en su caso, indique el interesado a efectos de notificaciones. Este domicilio no se tendrá en cuenta si el denunciado tuviese asignada una DEV.

b) **Sobre la infracción:** una descripción del hecho (especificando el lugar, fecha y hora) y la infracción presuntamente cometida.

c) **Sobre el denunciante:** el nombre y domicilio del denunciante (o, en su caso, el número de identificación profesional del Agente).

d) **Sobre la sanción:** El órgano competente para imponer la sanción y la norma que le atribuye tal competencia, la sanción que pudiera corresponder y el número de puntos cuya pérdida lleve aparejada la infracción.

e) **Sobre las acciones posibles:** Si el denunciado procede al abono de la sanción en el acto deberá señalarse, además, la cantidad abonada y las consecuencias derivadas del pago. En caso contrario, deberá indicarse que dicha denuncia inicia el procedimiento sancionador y que dispone de un plazo de veinte días naturales para efectuar el pago, con la reducción y las consecuencias establecidas en el artículo 80, o para formular las alegaciones y proponer las pruebas que estime convenientes. En este caso, se indicarán los lugares, oficinas o dependencias donde puede presentarlas.

3 PROTOCOLO DE NOTIFICACIÓN ELECTRÓNICA A TRAVÉS DE TECNOLOGÍAS ITS

En esta Sección se propone un protocolo para el envío de una notificación utilizando las tecnologías ITS. En primer lugar, se describe el modelo considerado (Sección 3.1.). En base a ese modelo, se definen una serie de requisitos que debe satisfacer el protocolo que se

[3] La Ley 18/2009 especifica que este contenido corresponde a las denuncias que los Agentes notifiquen en el acto al denunciado. No obstante, se asume que el contenido de la notificación que no se entregue en el momento contiene la misma información, pues causa el mismo efecto en el procedimiento.

propone (Sección 3.2.) basados en el marco legal presentado en la Sección 2. La arquitectura considerada se presenta en la Sección 3.3. Finalmente, la Sección 3.4 define el contenido de los mensajes a intercambiar y la Sección 3.5 muestra en detalle el protocolo propuesto.

3.1 Modelo

El modelo considerado en este trabajo se describe en la Figura 3.

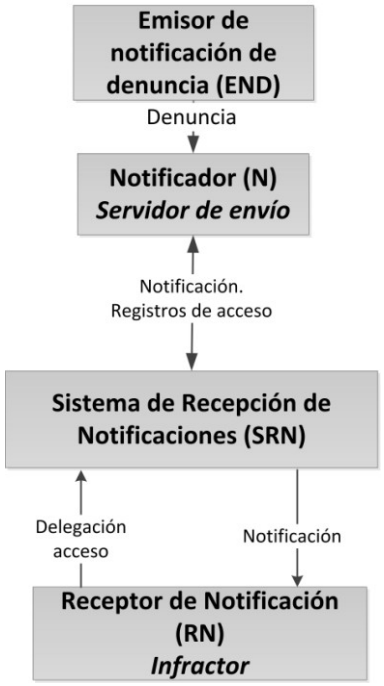

Figura 3. Modelo considerado en este trabajo

Existen dos diferencias con respecto al modelo que sustenta los mecanismos actuales (cf. Figura 2). En primer lugar, el Sistema informativo de Notificación ha sido eliminado, en tanto que la finalidad de esta entidad era el envío de un mensaje informativo advirtiendo sobre la existencia de notificación. Dado que el objetivo del trabajo previsto es transmitir, de manera inmediata, dicha notificación, la utilidad del SiN desparece. En segundo lugar, se introduce una nueva entidad, denominada Sistema de Recepción de Notificaciones (SRN), entre el Notificador (N) y el Receptor de Notificación (RN). Gracias al SRN, el RN (es decir, el infractor) no tiene que participar activamente en el protocolo propuesto, sino que delega en dicha entidad para que actúe en su nombre. Esta decisión se basa, por un lado, en el concepto de “interceptor” propuesto anteriormente por Robinson [10] y, por otro, en la

posibilidad de que sea “el interesado o su representante” la entidad que reciba la notificación, de acuerdo a la Ley 30/92 [8].

3.2 Requisitos

A la vista del marco legal general de la notificación electrónica (Sección 2.3) y del específico para el ámbito del tráfico (Sección 2.3.1), es posible establecer los requisitos que se deben exigir a dicho protocolo usando como base las exigencias impuestas a los mecanismos actuales. La Tabla 1 describe los requisitos, así como el precepto legal que lo motiva. En lo sucesivo, cada uno de los requisitos se denomina Req*i*, siendo *i* el número secuencial de requisito.

Identificador	Descripción	Origen
Req1	**Acreditación de disponibilidad:** N debe conocer fehacientemente el momento en que SRN ha recibido M	Art. 77.2 Ley 18/2009
Req2	**Acreditación de acceso:** N debe conocer fehacientemente el momento en que RN ha accedido a M	Art. 77.2 Ley 18/2009 (Art 7.2 Orden PRE-878-2010)
Req3	**Control de acceso autenticado a SRN:** Exclusivamente RN puede acceder a SRN	Art. 35.2 R.D. 1671/2009 (Art. 38.1 RD 1671-2009)
Req4	**Disponibilidad del sistema de notificación**: Tanto N como SRN deberán estar disponibles para el envío de M	Art. 9 Orden PRE-878-2010 (Art. 38.1 RD 1671-2009)
Req5	**Control de acceso físico**: Tanto N como SRN deberán disponer de elementos que protejan su acceso físico	Art. 8 Orden PRE-878-2010
Req6	**Sincronización**: Tanto N como SRN deberán estar sincronizados	Art 7 Orden PRE-878-2010

Identificador	Descripción	Origen
Req7	**Autenticación de M**: RN debe poder verificar que M fue creado por END	Art 5 Orden PRE-878-2010
Req8	**Confidencialidad de M**: Ninguna entidad distinta de END, SRN y RN puede conocer M	Art. 6 Orden PRE-878-2010
Req9	**Integridad de M**: El mensaje M recibido por RN debe presentar el mismo contenido que el mensaje creado por END	Art 5 Orden PRE-878-2010

Los requisitos Req1—Req6 afectan al *sistema de notificación*, mientras que los requisitos Req7—Req9 afectan al mensaje notificado (denominado *M*). Es preciso destacar que, de acuerdo al modelo planteado (Sección 3.1), el sistema de notificación se compone tanto de N como de SRN, ya que ambos se encargan de transmitir el mensaje entre el emisor y su receptor.

La acreditación del momento en que la notificación queda disponible al denunciado (Req1), y la del momento del acceso a su contenido (Req2), son exigencias que aparecen directamente en la Ley 18/2009. Una cuestión importante es si se debe acreditar “el acceso” o “el acceso por parte del interesado (e.d. RN)”. Dada la sensibilidad de la información en juego, y sabiendo que al menos para la dirección electrónica habilitada se necesita acreditar “el acceso del destinatario al contenido”, parece inevitable optar por la segunda opción. De hecho, esta necesidad motiva el requisito de que exista control de acceso autenticado sobre SRN, que es la parte del sistema de notificación con la que RN se relaciona (Req3). Esta necesidad se completa con el control de acceso físico que se debe imponer sobre el conjunto del sistema de notificación (Req5) que, en todo caso, deberá asegurar su disponibilidad (Req4). La necesidad de la acreditación temporal (expuesta en los requisitos Req1 y Req2) implica, además, que el sistema de notificación en conjunto esté sincronizado (Req6).

Con respecto a la seguridad de la información en juego, el ciudadano debe poder verificar que la notificación es auténtica. Dicha autenticidad se manifiesta en que el mensaje sea emitido por la entidad correspondiente (Req7) y que no haya sido modificado desde su creación (Req9). Además de lo anterior, dada la sensibilidad de la información en juego es

preciso garantizar que ningún tercero no autorizado pueda acceder a la información (Req8). A este respecto, la Orden PRE-878-2010 establece que el prestador de servicio de dirección electrónica no pueda acceder al contenido de los actos notificados. Trasladando esta necesidad al modelo considerado, debe exigirse que el Notificador no pueda acceder al mensaje – el Sistema de Recepción de Notificaciones, dado que debe presentárselo al legítimo Receptor RN, deberá conocerlo de forma imprescindible.

3.3 Arquitectura

Existen dos posibles arquitecturas del sistema basadas en el modelo anterior, y que aparecen reflejadas en las Figura 4 y Figura 5. La diferencia entre ambas estriba en la existencia de una entidad conocida como Autoridad de Resolución de Disputas (ARD), que actúa como tercera parte confiable. Las Secciones 3.3.1 y 3.3.2 presentan los aspectos comunes de ambas arquitecturas (la realización de las entidades y los canales de comunicación). La Sección 3.3.3 selecciona la alternativa más adecuada y la Sección 3.3.4 define, para la arquitectura escogida, el modelo de interacción a utilizar (en base a los definidos en la Sección 2.4.1).

3.3.1 Realización de las entidades

Con respecto a la realización de las entidades, el Notificador queda implementado a través de la infraestructura de RSU disponible en los sistemas ITS (ver Sección 2.1). Se asume que cada una de las RSU dispone de capacidad suficiente como para enviar los mensajes que se produzcan en el protocolo. Por su parte, el Sistema de Recepción de Notificación se realiza en una plataforma de computación en el vehículo que se organiza en base a la arquitectura OVERSEE (ver Sección 2.1). En esta entidad, se asume que el dispositivo de seguridad hardware almacena una clave privada asociada con el propietario del vehículo, y para cuyo uso es imprescindible la introducción de una contraseña. Dicha contraseña es conocida tanto por el propietario del vehículo como por sus conductores. El dispositivo de seguridad también almacena los certificados de clave pública del Emisor de Notificaciones de Denuncias (END) y, en su caso, de la Autoridad de Resolución de Disputas (ARD). En relación a estas entidades, ambos forman parte de la infraestructura del sistema de notificaciones y, por tanto, se implementan en nodos de computación con capacidad suficiente como para atender las tareas asignadas.

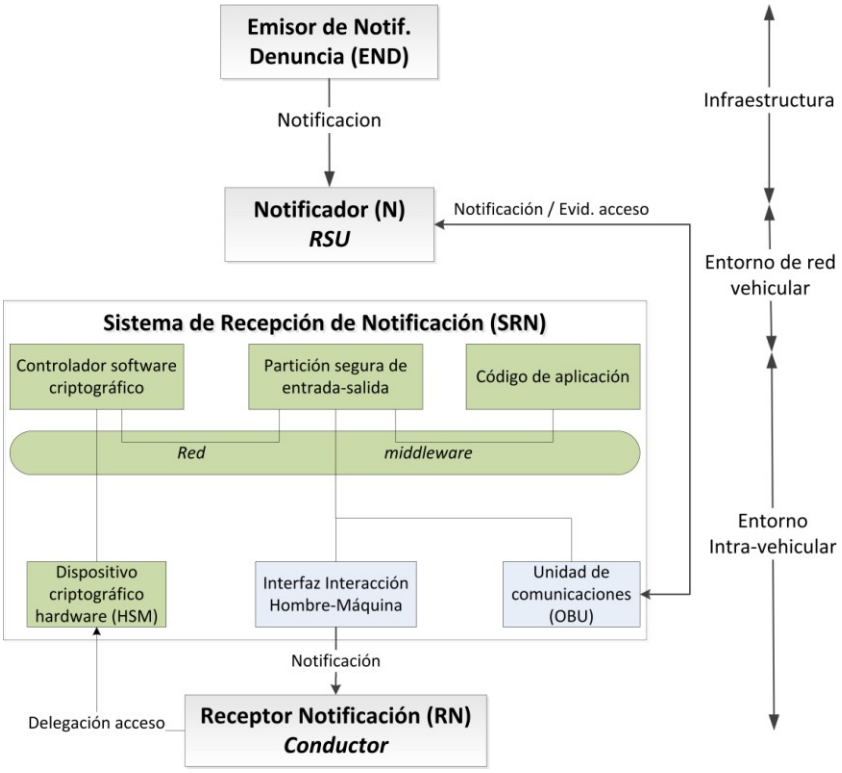

Figura 4. Arquitectura sin tercera parte confiable

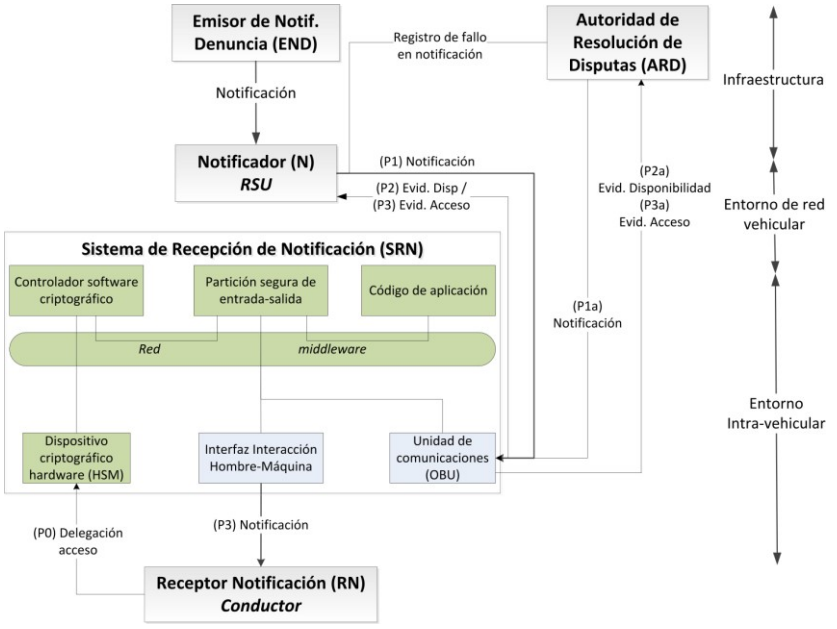

Figura 5. Arquitectura con tercera parte confiable, escogida en este trabajo

3.3.2 Canales de comunicación entre entidades

En las arquitecturas propuestas se distinguen tres entornos de red distintos: el de infraestructura, el de la red vehicular y el intra-vehicular. El entorno de infraestructura dispone de una comunicación entre entidades del cual se asume capacidad suficiente para procesar los mensajes intercambiados. Además, dado que se trata de la conexión entre entidades que, organizativamente, pertenecen a la Autoridad de Tráfico, se puede asumir que sólo las entidades autorizadas tienen acceso al sistema y que los mensajes transmitidos no pueden ser alterados en tránsito.

Por su parte, la conexión vehicular dispone de dos entornos distintos: la red basada en la tecnología DSRC (Sección 2.1.1) y la red inalámbrica disponible en espacios singulares (e.g. aparcamientos, estaciones de servicio). El perfil de la red DSRC es completamente contrario al presentado para el entorno de infraestructura: no garantiza la entrega de los paquetes, se trata de un medio compartido por todos los vehículos presentes en la región y los mensajes enviados pueden ser modificados por los nodos intermedios. Por su parte, la red de los espacios singulares se diferencia de la anterior en que la entrega de los paquetes está garantizada. Esto es debido a que, a pesar de ser también un medio inalámbrico y compartido, se asume que se dispone del tiempo suficiente como para gestionar los reenvíos necesarios hasta conseguir el envío efectivo de la información.

En base a los entornos vehiculares definidos, la conectividad entre el Notificador y el Sistema de Recepción de Notificación se realiza a través de la red DSRC, mientras que la conexión entre éste y la Autoridad de Resolución de Disputas (en su caso) se establece usando la red inalámbrica de los espacios singulares.

Por último, la red intra-vehicular se divide en dos grandes entornos: aquellos que se encuentran bajo la supervisión del dispositivo de seguridad hardware y los que no lo están (ver Sección 2.1.2). Así, mientras el primer entorno presenta el mismo perfil que la red de infraestructura, la conexión con la OBU y la interfaz hombre-máquina no garantiza que los paquetes intercambiados conserven su integridad.

3.3.3 Selección de arquitectura

La principal diferencia entre ambas arquitecturas radica en la existencia de una Autoridad de Resolución de Disputas (ARD), la cual vela por el desarrollo correcto del proceso en caso de que el Notificador no pueda completarlo satisfactoriamente. Para motivar su necesidad es

preciso tener en cuenta dos factores. En primer lugar, el canal de comunicación entre la RSU y la plataforma del vehículo no garantiza la entrega. En segundo lugar, tanto el dispositivo de comunicación del vehículo (OBU) como los postes de comunicación (RSU) pueden ser maliciosamente comprometidos. En estas circunstancias, si la notificación no se pudiera completar no sería posible determinar la causa: que se perdió el mensaje de notificación, el mensaje en el que se acusaba el recibo o que alguna de las entidades que decían haber enviado el mensaje realmente no lo hicieron [11]. Debe notarse que en este último caso, las consecuencias son distintas en función de la entidad que actúa incorrectamente. Si la RSU está comprometida, sería necesario proceder a su sustitución. En cambio, si se trata de la OBU, sería necesario llamar a revisión al dispositivo a fin de garantizar su buen funcionamiento no sólo para este servicio, sino para beneficio de las demás aplicaciones ITS. A la vista de este razonamiento, la arquitectura escogida en este trabajo es la que incorpora a la ARD (Figura 5).

3.3.4 Selección del modelo de interacción para la arquitectura seleccionada

Una vez establecida la arquitectura y, particularmente, la implementación de cada una de las entidades participantes, es posible determinar cuál de los modelos de interacción identificados en la Sección 2.4.1 es más adecuado para el contexto técnico considerado.

El modelo push exige que el Notificador (e.d. RSU) envíe de forma proactiva la notificación al SRN (e.d. la plataforma de computación del vehículo implicado). Para ello, es preciso conocer la localización de dicho vehículo. Sin embargo, el lugar de la infracción es conocido, por lo que en función del tiempo entre ésta y la notificación es posible estimar la localización (o posibles localizaciones) en la que se puede encontrar el vehículo. Por lo tanto, se podría resolver esta necesidad conjugando así mismo la debida protección de la privacidad, la cual se vería amenazada si fuera necesario efectuar un seguimiento constante de los vehículos [12].

Por su parte, el modelo pull exige que el vehículo, de forma periódica, consulte al Notificador por la existencia de nuevas notificaciones. En este sentido, es preciso señalar que los vehículos que cumplen las normas efectuarían constantemente estas consultas, sin que existiera nunca una notificación para ellos. Esto conllevaría una carga innecesaria en la red vehicular, que debe dar servicio a aplicaciones ITS con impacto en la seguridad vial. Por este motivo, en este trabajo se escoge el modelo push.

3.4 Definición de los mensajes a intercambiar

El protocolo de notificación propuesto persigue el intercambio de tres elementos de información: la *notificación*, la *evidencia de disponibilidad* y la de *acceso* al contenido. La notificación se estructura en base a los contenidos descritos en la Sección 2.5, y sobre los que se efectúan dos modificaciones (ver Tabla 2): por un lado, desaparece la dirección postal del infractor, ya que es el propio vehículo el lugar donde se practica esta notificación. Por otro, se añade la firma digital de la autoridad emisora del mensaje, a fin de garantizar la autoría y la integridad del mismo. Dado que el dispositivo de seguridad hardware ya almacena el certificado de clave pública del emisor del mensaje (necesario para verificar la firma), no es necesario adjuntarlo a la notificación.

La evidencia de disponibilidad (ver Tabla 3) contiene la huella del mensaje recibido (es decir, el resultado de aplicar una función resumen sobre el mensaje) y el momento en que esto sucede, firmado por la entidad correspondiente (en este caso, el dispositivo de seguridad hardware del vehículo). Para permitir al receptor verificar la firma, se adjunta el certificado de clave pública del firmante. La evidencia de acceso (Tabla 4) contiene, además de los elementos anteriores, la decisión que se toma en esta cuestión (aceptar o rechazar la notificación).

Tabla 2. Composición del mensaje de notificación y tamaño de sus campos

Grupo de datos	Elementos	Tamaño (bytes)
Infractor	Id. Vehículo	4
	Nombre del propietario	30
	Id. propietario	4
Infracción y sanción	Descripción	30
	Fecha	4
	Lugar	10
	Hora	2
	Órgano	20
	Norma	10
	Sanción	4
	Puntos	1
Denunciante	Id. dispositivo	4
Acciones	Consecuencias, explicación plazos, términos legales	100

Grupo de datos	Elementos	Tamaño (bytes)
Firma	Firma (S_{END}(campos anteriores))	56
	Certificado de clave pública	125
Tamaño total		**404**

Tabla 3. Composición del mensaje de evidencia de disponibilidad y tamaño de sus campos

Grupo de datos	Elementos	Tamaño (bytes)
Mensaje	Resumen (H(notificación))	32
Momento	Marca de tiempo	4
Firma	Firma (S_{HSM}(campos anteriores))	56
	Certificado de clave pública	125
Tamaño total		**217**

Tabla 4. Composición del mensaje de evidencia de acceso y tamaño de sus campos

Grupo de datos	Elementos	Tamaño (bytes)
Mensaje	Resumen (H(notificación))	32
Descripción del acceso	Marca de tiempo	4
	Decisión	1
Firma	Firma (S_{HSM}(campos anteriores))	56
	Certificado de clave pública	125
Tamaño total		**218**

3.5 Descripción del protocolo

El protocolo propuesto se describe en la Figura 6, empleando la notación (*Pi*) *A* → *B* : *m* para reflejar que la entidad *A* le envía a la entidad *B* el mensaje *m* en el paso *Pi*. La notación para los citados mecanismos criptográficos es la reflejada en la Tabla 1.

(P0) NR → HSM : Contraseña (HSM)

 # Los pasos P1 y P2 se repiten 'R' veces para promover su entrega al destinatario

(P1) END → RSU → OBU → HSM : E_{HSM} (Notif), siendo *Notif* la notificación según la Tabla 2

(P2) HSM → OBU → RSU : E_{RSU} (Evid.Disp), siendo *Evid.Disp* la evidencia de disponibilidad según la Tabla 3

SI(Mensaje (P2) no se recibe (e.d. RSU supera el tiempo de espera))

ENTONCES

 # Realizar este intercambio usando el canal de entrega confiable

(P1a) DRA → OBU → HSM : HSM : E_{HSM} (Notif), siendo *Notif* la notificación según la Tabla 2

(P2a) HSM →OBU → DRA : E_{DRA} (Evid.Disp), siendo *Evid.Disp* la evidencia de disponibilidad según la Tabla 3

SI(Mensaje (2a) no lo recibe DRA tras el tiempo de espera)

ENTONCES

 # El protocolo de notificación al vehículo no puede completarse DRA registra el incidente y comunica a la Autoridad de Tráfico para que se llame al vehículo a revisión. La notificación debe practicarse usando mecanismos tradicionales.

FIN-SI

(P3a) HMI → HSM → OBU → DRA : E_{DRA} (Evid.Acceso), siendo *Evid.Acceso* la evidencia de acceso según la Tabla 4

 # Si este paso no se produce antes del intervalo legal, la notificación se entiende como rechazada y el proceso continua (art. 77.2 Ley 18/2009)

FIN-SI

(P3) HMI →HSM → OBU →RSU : E_{RSU} (Evid.Acceso), siendo *Evid.Acceso* la evidencia de acceso según la Tabla 4

 # Si este paso no se produce antes del intervalo legal, la notificación se entiende como rechazada y el proceso continua (art. 77.2 Ley 18/2009)

Figura 6. Descripción del protocolo propuesto

El protocolo comienza (P0) con la delegación del conductor (Receptor de Notificación) en el dispositivo de seguridad hardware (elemento del Sistema de Recepción de Notificaciones) para que sea éste quien ejerza como su representante en el proceso de notificación. Para ello, se utiliza una contraseña que permite el uso de la clave privada, alojada en dicho dispositivo.

Una vez que se comete una infracción, la Autoridad (a través del Emisor de Notificación de Denuncias) prepara la notificación, que se envía a través de la RSU a la plataforma de computación del vehículo y, concretamente, hasta el dispositivo HSM (P1). Dicho dispositivo procede, en primer lugar, a descifrar el mensaje recibido, usando la clave privada alojada en él y cuyo uso fue autorizado por el conductor en el paso anterior. Tras esto, se procede a verificar la firma electrónica de la notificación y, en caso de que sea correcta, se prepara la evidencia de disponibilidad (P2). Para ello, se aplica una función resumen sobre el mensaje, y se introduce una marca de tiempo de esta operación usando la fuente de tiempo del propio dispositivo HSM. Toda esta información se firma empleando la clave privada alojada en dicho dispositivo.

Tras el acceso por el sistema a la notificación, es posible presentársela al conductor, para lo que se utiliza la interfaz hombre-máquina (HMI) integrada en la plataforma del vehículo. Cuando dicha presentación se produce (lo cual requiere encontrar el momento adecuado para que esta acción no interfiera con la labor de conducir), se prepara (P3) la evidencia de acceso reflejando la decisión del conductor (aceptar o rechazar la notificación). Debe notarse que si esta evidencia no se recibe en el plazo legal establecido (actualmente, 10 días según la Ley 18/2009), la notificación se entiende como practicada.

Los pasos anteriores se realizan utilizando la red vehicular basada en la tecnología DSRC. Cada uno de los envíos se repite un número *R* de veces para contrarrestar la eventual pérdida de información en la red vehicular. La Sección 4.2.1 analiza el valor adecuado del parámetro R. No obstante, si la evidencia de disponibilidad no se recibe en un período prefijado por parte de la RSU (Notificador), ésta delega en la Autoridad de Resolución de Disputas para que repita el paso P1 a través del canal de comunicación de los espacios singulares, cuya entrega es confiable. Esto da lugar a los pasos (P1a) para el envío de la notificación, (P2a) para el envío de la evidencia de disponibilidad y (P3a) para el envío de la de acceso. En el caso de que la ARD no obtenga la evidencia de disponibilidad en el plazo prefijado, se entiende que la plataforma del vehículo ha sido comprometida o funciona de manera incorrecta. En este caso, el protocolo de notificación se considera fallido y deberá realizarse empleando otros medios tradicionales. Además de esto, la ARD procedería a llamar a revisión al vehículo afectado, a fin de rehabilitar la plataforma.

4 ANÁLISIS DEL PROTOCOLO PROPUESTO

El análisis de la propuesta se realiza en dos vertientes. En primer lugar, la Sección 4.1 analiza el cumplimiento de los requisitos definidos en la Sección 3.2. En segundo lugar se estudia el rendimiento del protocolo en un entorno vehicular, teniendo en cuenta las capacidades tecnológicas de los sistemas ITS (Sección 4.2). En particular, dicho estudio se centra en analizar el tiempo necesario para conseguir que la notificación quede disponible para el infractor. Dicho tiempo (denominado $t_{ejecucion}$) será la suma del tiempo que emplea la Autoridad en preparar la notificación ($t_{procAuto}$) y el tiempo empleado por el protocolo para enviarla ($t_{protocolo}$) (Figura 7).

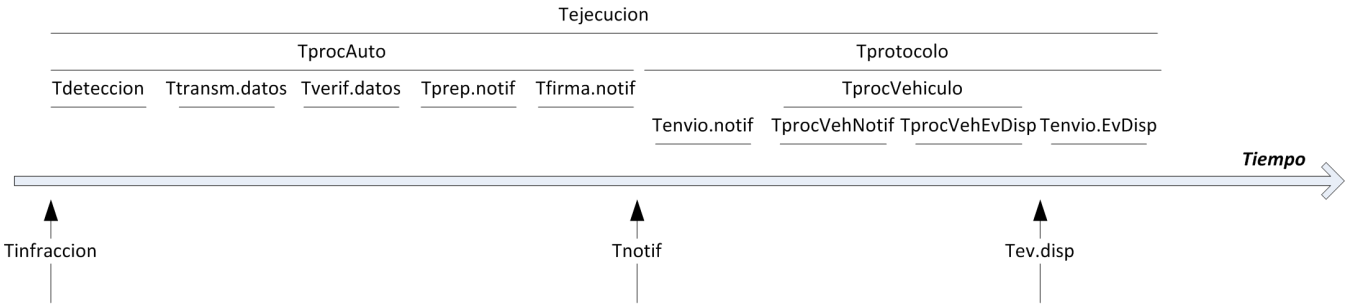

Figura 7. Evolución temporal del proceso considerado

Dado que, desde el punto de vista de la Autoridad, la eficacia del proceso se establece en función de su duración global (siendo más eficaz cuanto menor sea $t_{ejecucion}$), este análisis pretende caracterizar $t_{protocolo}$ con el fin de mostrar su grado de flexibilidad para conseguir el antedicho objetivo. La Sección 4.2 analiza $t_{protocolo}$, limitándose al escenario de red vehicular y sólo considerando el envío de la notificación (paso P1) y de la evidencia de disponibilidad (P2). La interacción con la ARD y el envío de la evidencia de acceso quedan fuera del alcance de este análisis ya que en ambos casos existe un tiempo de espera que puede ser muy superior al necesario para ejecutar los pasos analizados. En el primer caso, dicho tiempo de espera es el necesario para llegar a uno de los espacios singulares donde exista la conectividad prevista. En el segundo caso, el tiempo de espera es el que transcurre hasta que el conductor accede a la notificación, lo cual puede y debe producirse cuando esta acción no interfiera con la labor de conducir.

4.1 Análisis del cumplimiento de los requisitos impuestos

Con respecto a la entrega de la notificación, a la finalización del protocolo, existen tres estados posibles: que la notificación se haya puesto a disposición a través de la red vehicular, que haya sido necesaria la intervención de la Autoridad de Resolución de Disputas o que no haya sido posible entregarla. En los tres casos, la entidad

correspondiente dispone de los elementos necesarios para acreditar la situación. Si se entregó a través de la red vehicular, el Notificador dispone de la evidencia de disponibilidad que, al contener la firma electrónica del Sistema de Recepción de Notificación, atestigua que esa entidad accedió a ese mensaje en el momento indicado. Si intervino la ARD, será ésta quien disponga de este elemento de información y, si no pudo culminar la entrega, dado que la ARD es una entidad confiable y el canal que le unía con el SRN aseguraba la entrega del mensaje, esta entidad tiene potestad para registrar el evento de forma confiable. Así, el requisito Req1 queda satisfecho.

Una situación similar ocurre con la acreditación de acceso (Req2). La principal diferencia radica en que en este caso sólo hay dos opciones: si el Notificador o la ARD no la reciben en un plazo legal establecido, la propia Ley define que la notificación se ha practicado satisfactoriamente.

Con respecto al control de acceso autenticado al SRN (Req3), queda satisfecho ante la necesidad de introducir una contraseña (en el paso P0) para utilizar la clave privada alojada en el dispositivo de seguridad hardware. La propia seguridad del dispositivo garantiza que sólo al introducir esta contraseña se autoriza dicho acceso. No obstante, en sentido estricto, el mecanismo propuesto sólo garantiza que “alguien que conocía la contraseña” accedió al mensaje. Sería necesario introducir mecanismos de autenticación adicionales (específicamente, biométricos) para garantizar que dicha persona es el infractor. Este aspecto queda identificado como una línea futura de trabajo.

La disponibilidad del sistema de notificación (Req4) no puede darse por satisfecha sin un análisis práctico en una plataforma real. Si bien el Notificador debe estar disponible (bajo el supuesto de recursos suficientes de las RSU, ver Sección 3.3.1), ni la comunicación entre N y SRN, ni el propio SRN, actúan bajo esa suposición. El análisis del rendimiento del protocolo (Sección 4.2.1) persigue ilustrar esta discusión. Tampoco queda asegurado en el plano teórico el cumplimiento del control de acceso físico (Req5). Particularmente, mientras que la plataforma de computación vehicular dispone de una protección física intrínseca (al estar alojada en el interior del vehículo), las RSU están dispuestas en espacios públicos y accesibles, por lo que es necesario integrar dichas protecciones teniendo en cuenta esta circunstancia.

Con respecto a la sincronización del sistema de notificación (Req6), tanto el Notificador como el SRN disponen de una fuente fiable de tiempo accesible. El Notificador puede

acceder a ella (por ejemplo, el servidor de tiempo del Real Observatorio de la Armada) a través de la red de la infraestructura, mientras que la plataforma del vehículo dispone de ella gracias al dispositivo de seguridad hardware (HSM).

La autenticación del mensaje notificado (Req7) está asegurada gracias al uso de la firma electrónica sobre dicho mensaje, el cual asegura que el END es su emisor. Dicho mecanismo, tal y como se expuso en la Sección 2.2, también permite verificar la integridad del mensaje (Req9). Por su parte, la confidencialidad de este mensaje (Req8) queda garantizada por el uso de cifrado de clave pública. Es preciso destacar que el Notificador no puede acceder al mensaje ya que el cifrado lo realiza directamente el END en el paso P1.

4.2 Análisis del rendimiento

El tiempo de ejecución del protocolo ($t_{protocolo}$) se compone de tres factores principales (ver Figura 7): el tiempo para enviar la notificación ($t_{envio.notif}$), el tiempo requerido por el vehículo para procesar la notificación y preparar la evidencia de disponibilidad ($t_{procVehiculo}$), y el tiempo para enviar esta evidencia ($t_{envioEvDisp}$). Así,

$$t_{protocolo} = t_{envio.notif} + t_{procVehiculo} + t_{envioEvDisp} =$$
$$= t_{envio.notif} + t_{procVehNotif} + t_{procVehEvDisp} + t_{envioEvDisp}$$

En general, el tiempo de envío viene determinado por el tiempo necesario para transmitir un mensaje, así como de gestionar sus reenvíos para incrementar la probabilidad de que llegue a su destino a través de canales que no aseguren la entrega. Por su parte, el tiempo de procesamiento en la plataforma del vehículo viene determinado por su capacidad computacional. A continuación se analiza el tiempo de envío de los mensajes (Sección 4.2.1). Posteriormente se estudia el tiempo de procesamiento de la plataforma vehicular (Sección 4.2.2).

4.2.1 Cálculo de $t_{envio.notif}$ y $t_{envioEvDisp}$

Para combatir la falta de confiabilidad del canal vehicular, tanto la notificación como la evidencia de disponibilidad se reenvían *R* veces. El número de repeticiones R se establece de acuerdo a la probabilidad de éxito p_{exito} que se quiera alcanzar, dado que a mayor número de repeticiones, mayor probabilidad de que el mensaje alcance su destino (siempre que la probabilidad de entrega de un paquete no sea nula). Para las fases del protocolo

analizado, el éxito se alcanza cuando se transmiten correctamente tanto la notificación como la evidencia de disponibilidad. Al ser hechos independientes y sujetos a sus respectivas probabilidades, se tiene que $p_{exito} = p_{rcv.notif} \cdot p_{rcv.evDisp}$. En este análisis se asume que ambas probabilidades de transmisión son iguales (genéricamente llamadas $p_{rcv.mensaje}$), por lo que $p_{exito} = p_{rcv.mensaje}^2$.

$P_{rcv.mensaje}$ refleja la probabilidad de que al menos uno de los reenvíos llegue. De acuerdo a [13], la pérdida de paquetes en una red vehicular se produce de forma independiente con una probabilidad $p_{perdida}$, por lo que la mencionada probabilidad se calcula por la siguiente expresión:

$p_{rcv.mensaje} = 1 - (1- p_{perdida})^R = \sqrt{p_{exito}}$,

de lo que se puede establecer la relación entre el número de reenvíos y la probabilidad de éxito teniendo en cuenta la probabilidad de pérdida de un paquete:

$R = \log(1-\sqrt{p_{exito}}) / \log(1- p_{perdida})$

De acuerdo a [13], $p_{perdida} = 0.42$ para una comunicación vehículo-vehículo a una distancia de 400 metros[4]. Empleando este dato es posible observar la evolución del número de repeticiones en función de la probabilidad de éxito establecida (Figura 8). Así, para una probabilidad de éxito de 99,99%, es preciso reenviar el mensaje 18,18 veces, mientras que para una probabilidad del 75%, es suficiente con hacerlo 3,7 veces.

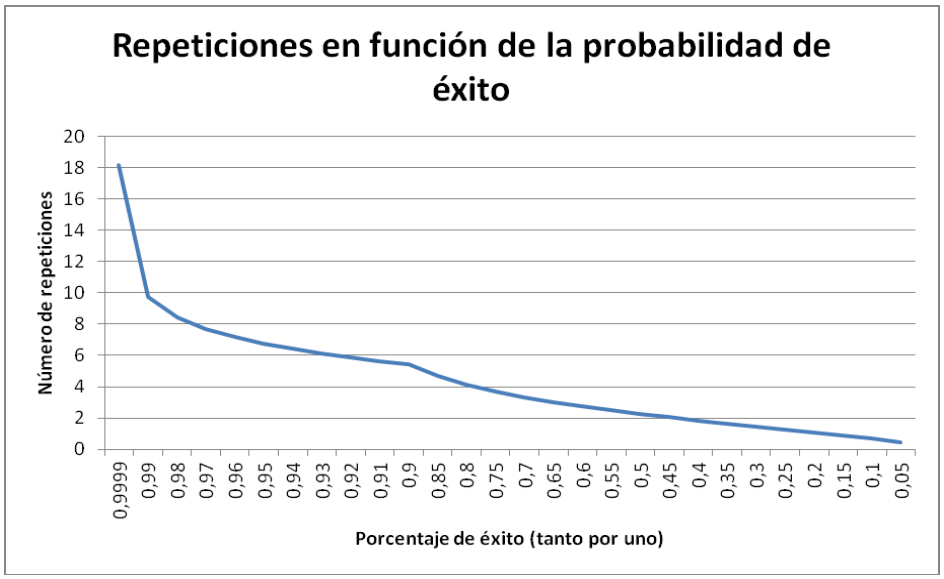

Figura 8. Evolución del número de repeticiones en función de la probabilidad de éxito

[4] A pesar de que la comunicación en este escenario es vehículo-infraestructura, se considera este indicador válido para ilustrar la fiabilidad esperada de dicha comunicación.

Empleando el número de reenvíos establecido, es posible determinar el tiempo total necesario para enviar cada uno de los mensajes considerados. Dicho tiempo se calcula como la suma de los tiempos de efectuar la transmisión de cada reenvíos[5], dando lugar a las siguientes expresiones:

$t_{envio.notif} = R \cdot t_{transm.notif}$ y

$t_{envio.EvDisp} = R \cdot t_{transm.EvDisp}$

El tiempo de transmisión de cada mensaje ($t_{transm.notif}$ y $t_{transm.EvDisp}$) viene determinado por su tamaño y la velocidad del canal. Las Tabla 2 y Tabla 3 describen el tamaño de ambos mensajes. Por su parte, la velocidad de transmisión más utilizada en los Estados Unidos para el canal DSRC es de 6 Mbps [14]. Empleando ambos datos, el tiempo de efectuar los reenvíos (en función, nuevamente, de p_{exito}) queda reflejado en la Figura 9. Así, para una probabilidad de éxito de 99,99%, se emplean 0,0098 segundos en transmitir la notificación y 0,0053 segundos en la evidencia de disponibilidad.

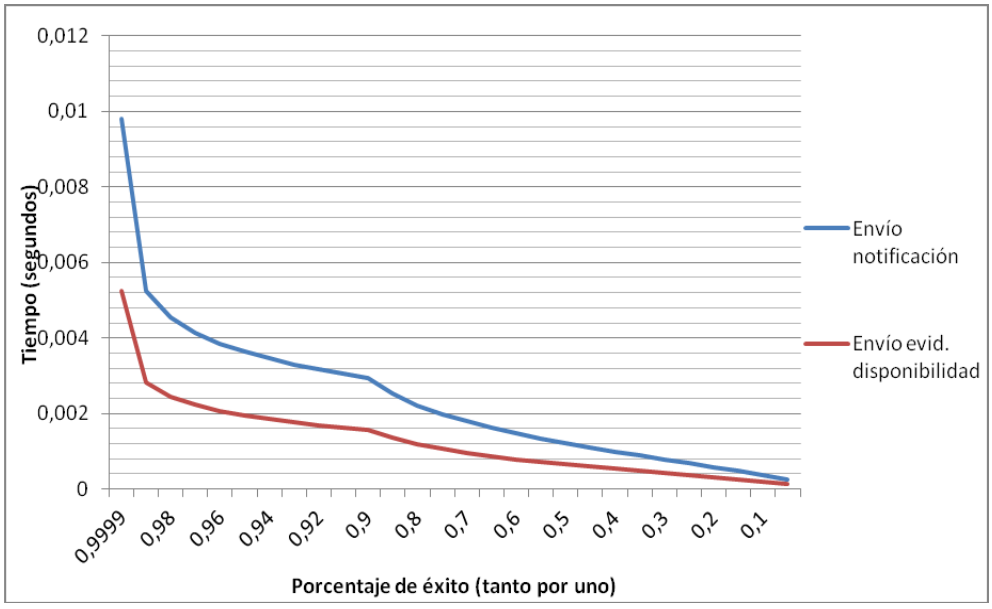

Figura 9. Tiempo de envío de los mensajes considerados en función del porcentaje de éxito

4.2.2 Cálculo de $t_{procVehNotif}$ y $t_{procVehEvDisp}$

Las tareas computacionalmente más significativas por parte del vehículo residen en la realización de cálculos criptográficos. Así, se considera que otras tareas (encolado de

[5] Este tiempo es el mínimo posible, ya que podrían existir retrasos entre reenvíos. En otras palabras, se está asumiendo que todos los reenvíos se pueden realizar de forma inmediata, es decir, que no existen tiempos de espera para utilizar el canal.

mensajes, descartar múltiples reenvíos recibidos, cambios de contexto para atender a otros servicios ITS, etc.) suponen un coste despreciable frente a los procesos criptográficos. En particular, el vehículo debe descifrar el mensaje de notificación y, con el resultado, verificar la firma para comprobar su integridad y autenticidad. Con respecto al mensaje de evidencia de disponibilidad, el vehículo debe firmarlo electrónicamente para garantizar su autenticidad, así como cifrarlo para su destinatario.

Para ilustrar el tiempo que requieren las antedichas operaciones, se ha considerado el rendimiento ofrecido por una plataforma de computación vehicular (CycurV2X) [15]. Dicha plataforma efectúa el cifrado de 16 bytes en 27,938 ms (21,26 ms. para el descifrado). Por su parte, la firma de dicha información se realiza en 7,156 ms (empleando 27,114 ms. para su verificación).

Los mensajes que se gestionan en este contexto son significativamente más grandes que los considerados en los parámetros de rendimiento. Así, es preciso extrapolar los parámetros anteriores para la longitud del mensaje considerada. El método de extrapolación depende de la naturaleza del algoritmo. En el caso del cifrado, el algoritmo ECIES consiste en un cifrado de flujo utilizando una clave que se cifra mediante cifrado asimétrico. Así, la operación más costosa es dicho cifrado asimétrico y se estima que el coste del cifrado de flujo es proporcional (lineal) a la longitud del mensaje. Por el contrario, el algoritmo de firma ECDSA cifra asimétricamente el resultado de aplicar una función resumen al mensaje en cuestión. Dado que, por definición, el resultado de una función resumen tiene siempre la misma longitud con independencia de la del mensaje original, la diferencia de longitud del mensaje afecta exclusivamente a la realización de la función resumen. Dicha función resumen (SHA-256, en este trabajo) divide los mensajes en bloques de 64 bytes. Así, el impacto viene dado por la diferencia de longitudes medida en múltiplos del tamaño de bloque.

A la vista del razonamiento anterior, el procesamiento del mensaje de notificación requiere
$t_{procVehNotif} = t_{descifrarNotif} + t_{verifNotif}$ = 21,26 (*ms / bloque de 16 bytes)*· $ratio_{descif}$ + 27,114 *(ms / bloque de función resumen)* · $ratio_{verif}$, siendo
$ratio_{descif}$ = 404 bytes (notif) / 16 bytes (implementación referencia) = 25,25 *bloques de 16 bytes*
$ratio_{verif}$ = 223 bytes a verificar (notif) / 64 bytes por bloque de función resumen = 4 bloques de función resumen.

Empleando estos datos en la expresión anterior, se tiene que

$t_{procVehNotif} = t_{descifrarNotif} + t_{verifNotif} = 21{,}26 \cdot 25{,}25 + 27{,}114 \cdot 4 = 645{,}271$ ms = 0,645 s.

De forma análoga,

$t_{procVehEvDisp} = t_{firmarEvDisp} + t_{cifrarEvDisp} =$

$= 7{,}156$ (*ms / bloque de función resumen)*$\cdot ratio_{firma} +$

$+ 27{,}938$ *(ms / bloque de 16 bytes bloque de función resumen)* $\cdot ratio_{cifrado}$,

siendo en esta ocasión

$ratio_{firma}$ = 36 bytes a firmar (ev. disponibilidad) / 64 bytes por bloque de función resumen = 1 (ya que no se puede procesar menos de un bloque)

$ratio_{cifrado}$ = 217 bytes (notif) / 16 bytes (implementación referencia) = 13,56 *bloques de 16 bytes*

Usando estos valores, se puede calcular el tiempo definitivo para la evidencia de disponibilidad,

$t_{procVehEvDisp} = 7{,}156 \cdot 1 + 27{,}938 \cdot 13{,}56 = 386{,}065$ ms = 0,386 s.

Empleando los valores de $t_{procVehNotif}$ y $t_{procVehEvDisp}$, es posible calcular el tiempo total que invierte el vehículo en la computación de los mensajes, $t_{procVehiculo} = t_{procVehNotif} + t_{procVehEvDisp} = 0{,}645 + 0{,}386 = 1{,}031$ s.

5 TRABAJOS RELACIONADOS

En el ámbito de las redes vehiculares, existen un número significativo de aplicaciones ITS que, como la notificación considerada, requieren que (1) el mensaje llegue al vehículo y (2) se pueda demostrar esta circunstancia con vistas a una posible resolución de disputas. A continuación se analizan dos ejemplos de dichas aplicaciones.

En primer lugar, la transmisión electrónica de las señales de tráfico al vehículo ha sido identificada como potencialmente beneficiosa, especialmente para la mejora de la seguridad vial de los conductores de edad avanzada [16]. En el escenario futuro en que las señales se transmitieran exclusivamente de esta forma, acreditar que el vehículo recibió la información sería suficiente para sancionar a los conductores que no cumplieran la norma. En segundo lugar, la aplicación EDA (del inglés *Enhanced Driver Awareness*, Concienciación mejorada

del conductor) permite que el conductor reciba información sensorial de otros vehículos y elementos de la infraestructura. Así, dispone de conocimiento sobre más allá de lo que visualmente puede alcanzar [17]. Nuevamente, si el conductor toma una decisión que resulta en un incidente de tráfico, y dicha decisión entra en conflicto con los datos recibidos a través de EDA, la culpa atribuible al conductor podría ser mayor que la que correspondería ante un hecho fortuito.

A pesar de la descripción anterior, hasta donde alcanza el conocimiento de los autores ninguna de las contribuciones sobre estas aplicaciones ha considerado los escenarios de que el mensaje no llegue al destinatario o que no se obtenga el debido acuse de recibo por parte del vehículo. Este trabajo considera ambas cuestiones en el diseño del protocolo gracias a la incorporación de una tercera parte de confianza con la que existe una conexión de entrega confiable. No obstante, debe notarse que el uso de dicho canal se produce, previsiblemente, tras un lapso significativo de tiempo. A diferencia de lo que ocurre con la notificación, dicho lapso anularía la utilidad de las aplicaciones comentadas. Así, la transmisión de una señal de tráfico vigente en un tramo anterior o los datos de la aplicación EDA correspondientes a un escenario ya pasado carecerían de utilidad para el conductor.

6 CONCLUSIONES Y LÍNEAS FUTURAS

Los mecanismos actualmente existentes para el envío de la notificación permiten que el infractor conozca la existencia de la sanción varios días después de la ocurrencia del hecho. Incluso empleando medios electrónicos, dicho conocimiento podría producirse, como pronto, una vez finalizado el viaje. Esta circunstancia afecta negativamente al poder educativo de la sanción. Para contribuir a esta cuestión, en este trabajo se ha presentado un protocolo de envío de la notificación al vehículo utilizando tecnologías ITS. Para que dicho mecanismo pueda ser legalmente admisible, se han impuesto una serie de requisitos derivados de los que se exigen para los mecanismos actualmente regulados. Se ha analizado el cumplimiento de dichos requisitos por parte del protocolo propuesto, concluyéndose que se satisfacen todos aquellos que pueden verificarse con independencia de su implementación concreta. Por otro lado, para verificar la adecuación de la propuesta a un entorno vehicular, se ha analizado su coste tanto para la red de comunicación vehicular como para los dispositivos de computación del vehículo. El análisis se ha centrado en el intercambio de la notificación y la evidencia de disponibilidad, concluyendo que se emplean 0,0098 segundos en transmitir la notificación (con una probabilidad de éxito del 99,99%), 0,645 s. en

procesarla, 0,386 s. en preparar la evidencia de disponibilidad y 0,0053 s. en transmitirla (con la misma probabilidad de éxito).

Las líneas futuras pasan, en primer lugar, por integrar este proceso con un futuro proceso de detección de la denuncia en el que, gracias a la tecnología ITS, sea posible identificar al conductor que verdaderamente comete la infracción. El mismo mecanismo podrá adaptarse para asegurar que el que recibe la notificación es la persona infractora. Además de lo anterior, se debe completar el análisis presentado en este trabajo, a fin de verificar si las redes inalámbricas existentes en los espacios singulares cumplen la suposición de entrega asegurada. Igualmente, debe estudiarse experimentalmente el tiempo medio de ejecución del protocolo teniendo en cuenta la duración típica del viaje, en distintos entornos (urbano, interurbano, autopista).

AGRADECIMIENTO

Este trabajo ha sido realizado en el marco del proyecto E-SAVE, subvencionado por el Ministerio de Ciencia e Innovación (referencia TIN2009-13461).

BIBLIOGRAFÍA

[1] COMISIÓN EUROPEA (2010). “Directiva 2010/40/ue del Parlamento europeo y del Consejo, de 7 de julio de 2010, por la que se establece el marco para la implantación de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte”, Diario oficial de la UE.

[2] ESPAÑA (2009). “Ley 18/2009, de 23 de noviembre, por la que se modifica el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 339/1990, de 2 de marzo, en materia sancionadora”. Boletín Oficial del Estado (BOE).

[3] ESPAÑA (2009). “Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos”. Boletín Oficial del Estado (BOE).

[4] MÄKINEN, T., ZAIDEL, D. et al (2003). “Traffic enforcement in Europe: effects, measures, needs and future”. ESCAPE project.

[5] ESPAÑA (2007). “Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.”. Boletín Oficial del Estado (BOE).

[6] KARGL, F. et al. (2008). “Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges”, IEEE Communications magazine.

[7] IEEE (2006). “1609.2: Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages”.

[8] ESPAÑA (1992). “Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común”. Boletín Oficial del Estado (BOE).

[9] ESPAÑA (2010). “Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre. Boletín Oficial del Estado (BOE).

[10] ROBINSON, P. (2005). “Middleware for fair non-repudiable interactions”, 6th Annual Postgraduate Symposium on the Convergence of Telecommunications.

[11] FERRER-GOMILLA, J.L. et al (2010). “Certified electronic mail: Properties revisited”. Computers & Security.

[12] HUBAUX, J.-P, CAPKUN, S., LUO, J. (2004) “The security and privacy of smart vehicles”, IEEE Security and Privacy.

[13] BAI, F., KRISHNAN, H. (2006). “Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications," IEEE Intelligent Transportation Systems Conference.

[14] KENNEY, J. B. (2011). “Dedicated Short-Range Communications (DSRC) Standards in the United States”. Proceedings of the IEEE.

[15] escrypt INC. (s.f.), “CycurV2X Technical details”, accesible en: https://www.escrypt.com/?id=51 (en inglés), accedido en Febrero de 2012.

[16] UNIVERSITY OF CALGARY (2006), “In-vehicle intelligent transportation system (ITS) countermeasures to improve older driver intersection performance”, accesible en: http://www.tc.gc.ca/eng/innovation/tdc-projects-its-a-5285-1204.htm , accedido en Febrero de 2012.

[17] KOVACS, A. et al. (2006) ”Use Cases and System Requirements (Deliverable 2.2)”, Cooperative Vehicle-Infrastructure Systems (CVIS) project.

[18] INT. STANDARDS ORGANIZATION (1989). “ISO 7498-2 Information processing system - Open systems interconnection - Basic reference model - Part 2: Security architecture.”