# PROYECTOS E-SAVE Y PRECIOUS SOBRE LA APLICACIÓN DE TECNOLOGÍAS ITS PARA LA SUPERVISIÓN DEL CUMPLIMIENTO DE NORMAS

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

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

**Almudena Alcaide Raya**
Doctora en Ingeniería Informática. Profesora Ayudante Doctor. Universidad Carlos III de Madrid

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

**RESUMEN:** En esta contribución se presentan la motivación y los principales resultados de los proyectos de investigación E-SAVE (Arquitectura de Seguridad y Generación de Pruebas Electrónicas Forenses en Entornos Vehiculares, financiado por el Ministerio de Educación y Ciencia, 2010-2012) y PRECIOUS (Privacidad Responsable en la Circulación de Vehículos, financiado por la Comunidad de Madrid, 2011). En ambos proyectos, y con la pretensión de repercutir beneficiosamente en la seguridad vial, se proponen sistemas de supervisión y gestión automatizada, inmediata y telemática de ciertos aspectos del tráfico rodado: el proceso sancionador administrativo, en el caso de E-SAVE, y la verificación privada de las autorizaciones requeridas para circular, en el caso de PRECIOUS.

## 1 INTRODUCCIÓN

Actualmente estamos inmersos en lo que se ha venido a denominar la sociedad de la información. Las tecnologías de la información y las comunicaciones (TIC) experimentan desde hace tiempo y de forma continuada una gran evolución. El principal objetivo hacia el que se dirigen es a proporcionar un acceso a la información de forma global, personalizada, en cualquier momento y desde cualquier lugar. Si, además, añadimos transparencia y adaptabilidad a dicho acceso, estamos enumerando los atributos fundamentales del

paradigma de la computación ubicua, tan en auge en la actualidad debido principalmente a su prometedora aplicación en los entornos móviles. De hecho, esta situación se ha reflejado recientemente en el sector del transporte, dando lugar a lo que se conoce como los sistemas inteligentes de transporte (ITS, del inglés Intelligent Transportation Systems) soportados por las denominadas redes vehiculares (VANETs, del término en inglés Vehicular Ad-hoc Networks). Brevemente, estas redes móviles y ad hoc suelen contemplar una infraestructura de comunicación entre los propios vehículos (V2V, del inglés vehicle-to-vehicle), y entre la infraestructura de carretera y los vehículos (R2V, road-to-vehicle). La introducción de las TIC en este ámbito está permitiendo ofrecer funcionalidades que antes no eran posibles como por ejemplo el cobro de peajes o de tasas de seguro (que se valoran, entre otras, en función del cumplimiento de las normas de tráfico por el conductor) [1] o, incluso, la automatización completa de la conducción de los vehículos mediante manejo remoto por parte de la infraestructura [2].

El grupo de investigación de seguridad en las tecnologías de la información y las comunicaciones[1] de la Universidad Carlos III de Madrid está llevando a cabo dos proyectos de investigación cuyo objetivo principal es utilizar los ITS y las VANETs para mejorar la supervisión y gestión de ciertas normas de tráfico. Estos proyectos son el proyecto E-SAVE (Arquitectura de Seguridad y Generación de Pruebas Electrónicas Forenses en Entornos Vehiculares, financiado por el Ministerio de Educación y Ciencia, 2010-2012) y el proyecto PRECIOUS (Privacidad Responsable en la Circulación de Vehículos, financiado por la Comunidad de Madrid, 2011). En ambos proyectos, y con la pretensión de repercutir beneficiosamente en la seguridad vial, se proponen sistemas de supervisión y gestión automatizada, inmediata y telemática de ciertos aspectos del tráfico rodado: el proceso sancionador administrativo, en el caso de E-SAVE, y la verificación privada de las autorizaciones requeridas para circular, en el caso de PRECIOUS. A continuación se expone el planteamiento de cada proyecto y las contribuciones a las que han dado lugar.

## 2 PLANTEAMIENTO

### 2.1 E-SAVE

Aunque el proyecto E-SAVE tiene también por finalidad la transmisión segura de información al conductor acerca del estado del tráfico y de las vías atendiendo al lugar donde éste se

[1] http://www.seg.inf.uc3m.es

encuentra, su principal objetivo es promover una gestión más eficaz de las denuncias mediante la propuesta de un sistema que permita su automatización utilizando las TIC. En efecto, el peso burocrático del procedimiento sancionador adecuado, junto con la demora para que la sanción adquiera firmeza hace que frecuentemente el proceso no tenga la eficacia prevista y carezca de la ejemplaridad derivada de su inmediata notificación. Teniendo en cuenta este problema, en diciembre de 2008 se presentó una propuesta de reforma de la Ley sobre Tráfico, que pretende introducir cambios en el procedimiento sancionador con vistas a simplificar el proceso [3]. Sin embargo, la reforma legal no resuelve de forma completa el problema pues presenta dos carencias fundamentales. Por un lado, sigue sin ser posible identificar fehacientemente al conductor del vehículo infractor, cuando se tiene conocimiento del hecho a través de medios de captación de imágenes. Esto hace posible que el propietario del vehículo identifique como conductor infractor a otra persona distinta, evitando así que el peso de la sanción recaiga sobre el conductor implicado. Además, en segundo lugar, el conductor no conoce la existencia de la sanción hasta que no recibe la notificación, hecho que se produce pasados varios días desde la comisión del hecho. Esto incide negativamente en la efectividad de la sanción y, además, constituye una vulneración del “derecho a conocer” el estado de tramitación de los procedimientos en los que se encuentra implicado, previsto por la legislación.

La utilización de las TIC en este ámbito permitiría una completa automatización del procedimiento de denuncia. Como antecedente significativo, en 2007 se creó en España el Centro de Tramitación de Denuncias Automatizadas (ESTRADA), por el cual se dota de la infraestructura de procesamiento necesaria para las infracciones de Tráfico [4]. Además, los agentes encargados de la vigilancia del tráfico han sido equipados con dispositivos tipo PDA que permiten consignar los datos de forma clara y enviarlos inmediatamente al citado centro. Estas medidas, aunque fortalecen el procedimiento sancionador y aumentan su capacidad de tramitación, no eliminan las carencias que se señalaron anteriormente. Un sistema basado en TIC que contribuyera a resolver esta necesidad debería integrar de forma coordinada todas las fases del proceso de denuncia. Consideremos, por ejemplo, que un vehículo circula a velocidad excesiva. El proceso comienza con la detección de la infracción por parte de los elementos de medición correspondientes (por ejemplo, sensores de velocidad dispuestos en la vía). Una vez detectada, se deben recoger y acreditar todos los elementos de prueba necesarios para la tramitación de la denuncia (vehículo infractor, conductor del mismo, lugar y tiempo de comisión de la infracción, así como velocidad aplicable si fuera variable, tal y como se propuso anteriormente). Finalmente, se debe

comunicar al vehículo en cuestión la existencia de la denuncia, promoviendo así una actitud de respeto hacia los preceptos del Código de Circulación.

Señalamos a continuación, muy brevemente la relevancia que tienen las Leyes vigentes sobre la factibilidad de un sistema de estas características. El procedimiento sancionador se rige por la legislación específica y, tras la reforma del Código Penal, existen delitos contra la seguridad del Tráfico que pueden conllevar penas de cárcel. Es por tanto fundamental asegurar que el diseño del proceso otorga las garantías necesarias para la validez del procedimiento. Dichas garantías comienzan en el aseguramiento de la información transmitida, es decir, garantizan su confidencialidad, integridad, autenticación y no repudio. Un aspecto que determina en gran medida las soluciones aplicables es el hecho de que el conductor tiene, en el caso de ser infractor, poco o ningún interés en participar en el proceso. Además, en caso de hacerlo, podrá tratar de falsificar su identidad o la información acerca de la infracción, para evitar la sanción. Por este motivo, el diseño del proceso debe realizarse de forma extremadamente cautelosa. La existencia de módulos de procesamiento confiables (TPM, del inglés Trusted Platform Module) permite atisbar que es posible delegar algunos aspectos al propio vehículo [5]. Inicialmente, es posible delegar en él la identificación del conductor (haciendo uso, por ejemplo, del Documento Nacional de Identidad Electrónico recientemente implantado en España) o la del propio vehículo (para lo que se han propuesto soluciones tipo PKI [6] o incluso estándares ISO [7]). Sin embargo, no existen modelos ni arquitecturas globales que hayan abordado la propuesta de un sistema que permita automatizar el proceso de denuncia, tanto en el plano nacional como internacional.

Un sistema de este tipo debería estar soportado por los mecanismos adecuados que permitan obtener evidencias irrefutables acerca del comportamiento de los vehículos. En la actualidad, existen mecanismos que permiten registrar el comportamiento por parte del propio vehículo. Es el caso, por ejemplo, de los dispositivos EDR (del inglés, Event Data Recorders) [8]. No obstante, los dispositivos incorporados al vehículo no están exentos de errores de medición y, además, el cableado interno del vehículo está expuesto a manipulaciones intencionadas [9]. Gracias a la utilización de las TIC en el ámbito vehicular, sería posible abordar el problema desde una nueva perspectiva; nos referimos a la obtención de evidencias electrónicas del comportamiento de los vehículos a través de los colindantes, además o de forma alternativa a las que se puedan obtener a través de los elementos de la infraestructura de carretera o a través de mecanismos implantados en el propio vehículo. De esta manera, se puede decir que se está extendiendo el rol tradicional

de “testigo” al ámbito vehicular. Gracias a este tipo de pruebas sería posible, por ejemplo, que los conductores y/o vehículos denunciados obtuvieran evidencias sobre su comportamiento que les permitiesen argumentar que se estaba actuando correctamente en el momento en que se registró una infracción (refutación de sanciones). Actualmente, si un conductor es denunciado por exceso de velocidad, los recursos se centran en comprobar si los dispositivos de medición han sido reglamentariamente verificados, pero no es posible demostrar que no se circulaba cumpliendo los límites de velocidad. Esta nueva forma de creación de evidencias forenses vehiculares (que denominamos Vehicular Ad-hoc Forensic Evidences o VAFEs) también podría aplicarse a la resolución de disputas por parte de las aseguradoras en caso de accidente o para generar evidencias testimoniales de atestados. Esto representa un avance significativo y totalmente novedoso en esta área. Por su parte, el estándar J2735 de SAE incluye un formato que define una posible estructura para la información que típicamente contendría una VAFE. Sin embargo, este estándar carece de elementos de información que permitan comprobar su origen y validez [10]. Además, no existe en la literatura ningún modelo que aborde la posibilidad de obtener evidencias de forma distribuida y multimodal en los entornos vehiculares a través de “testigos”.

En consonancia con lo expuesto, el proyecto E-SAVE tiene los siguientes objetivos:

1) Definición de un modelo de arquitectura para redes vehiculares que permita la transmisión de información de forma fiable entre los distintos agentes involucrados, así como la automatización y mejora de los procesos de denuncia.
2) Diseño de sistemas y protocolos para la transmisión segura de información fiable acerca del tráfico y de las vías.
3) Diseño de sistemas y protocolos para la automatización del proceso coordinado de gestión de denuncias que incluya los mecanismos de seguridad adecuados para poder garantizar la validez jurídica del procedimiento
4) Diseño de elementos y protocolos para la obtención de evidencias forenses vehiculares a través de la utilización de las TIC y su integración en el proceso de gestión de denuncias.
5) Validación de las soluciones propuestas mediante la implementación de un demostrador o a través de simulaciones.

### 2.2 PRECIOUS

El proyecto PRECIOUS tiene como principal finalidad la mejora de la eficacia de los procesos de detección de las autorizaciones requeridas para circular mediante la propuesta

de un sistema automático, telemático y respetuoso con la privacidad basado en el uso de tecnologías ITS y credenciales anónimas. El principal beneficio esperado es precisamente una mejoría de la seguridad vial, que hoy en día es uno de los mayores retos en los países desarrollados. En efecto, uno de los requisitos para circular es contar con las mencionadas credenciales válidas y actualizadas, que acrediten que las condiciones de los vehículos y sus conductores son las adecuadas desde el punto de vista de la seguridad vial. La vigilancia del cumplimiento de este requisito (impuesto como norma por las legislaciones en los diferentes países y objetivo estratégico en el EU Road Safety Program 2011-2020 [11]) se implementa habitualmente a través de patrullas desplegadas a lo largo de las carreteras. Los agentes deben parar a los vehículos e inspeccionar visualmente las credenciales, la mayoría de las cuales están en soporte papel o plástico. La efectividad de este procedimiento para reducir el número o la seriedad de los accidentes de tráfico depende directamente de la intensidad de los controles. Por tanto, circular sin unas credenciales válidas es ciertamente relevante desde el punto de vista de la seguridad vial. Sin embargo, las cifras demuestran que la situación actual dista bastante de la ideal. En España, se detectó que 400.000 vehículos estaban circulando sin haber pasado la inspección técnica obligatoria en 2009 [12] y en 2006 había 1.4 millones de vehículos sin seguro [13]. Más aún, se estima que la cantidad de vehículos que no habían satisfecho el impuesto de circulación en Reino Unido en 2006 era de 2.1 millones [14] y el proyecto Unlicensed drivers encontró que el 39% de los conductores que habían sido desprovistos de la licencia de conducción por acumulación de sanciones habían conducido sin dicha licencia [15].

La Comisión Europea está trabajando en el despliegue de estas credenciales en formato electrónico y ha sugerido que las tarjetas inteligentes sean el soporte físico que albergue las licencias de conducción [16, 17, 18]. La utilización de este tipo de credenciales electrónicas constituiría una significativa barrera para evitar la creación ilegal de credenciales y una oportunidad de aplicar nuevos y más eficientes mecanismos de supervisión de las normas de tráfico. Como ejemplo, la TISPOL (European Traffic Police Network) prevé que los futuros sistemas de identificación automática de conductores están basados en las licencias de conducción electrónicas [19]. En España, ya se ha diseñado y aprobado el formato electrónico de la tarjeta de inspección técnica de vehículos [20].

Los sistemas de vigilancia construidos utilizando sistemas de credenciales electrónicas y tecnologías ITS habilitarían una supervisión más conveniente, frecuente y efectiva. Sin embargo, este tipo de sistemas pueden alzar preocupaciones no desdeñables relativas a la privacidad, por la facilidad que tendrían las Administraciones u organismos responsables

para trazar a vehículos y conductores. Por tanto, de entre los sistemas de credenciales electrónicos existentes, son más idóneos aquellos que se denominan privados o anónimos.

La necesidad creciente de privacidad por parte de todos los participantes en una operación electrónica ha provocado un análisis crítico de los sistemas de credenciales más utilizados actualmente, es decir, aquellos basados en certificados de clave pública y certificados de atributos. El sujeto, al presentar dicho tipo de credenciales, no solo está acreditando su identidad real, sino también revelando parcial o totalmente otros atributos. Por ejemplo, en el DNIe, para acreditar la mayoría de edad, el atributo que se desvela es la fecha de nacimiento cuando sólo la "mayoría de edad" es el dato necesario. En el peor de los casos, el conjunto de atributos asociados ha de desvelarse al mismo tiempo (nombre, apellidos, género, fecha y lugar de expedición, huella dactilar, etc.)

Hoy en día podemos obtener identidades digitales menos intrusivas (cuentas de correo electrónico vía web, foros, redes sociales, etc.), creándose así identidades digitales formadas por todos aquellos datos y servicios utilizados por un único individuo, que se encuentran relacionados o pertenecen a Internet, y que identifican y definen al mismo dentro de la red. Estas identidades definidas anónimamente no revelan información sobre la identidad real de las personas o sujetos, pero impiden la trazabilidad de estos sujetos y la asignación de responsabilidades a partir de sus actividades en la red. Las directrices de seguridad de las tecnologías de la información son claras y están basadas en la trazabilidad de eventos y usuarios en un sistema por medio de ficheros de auditoría, registros de eventos y la autenticación de usuarios. Estos mecanismos atentan directamente contra la privacidad de los usuarios, aunque resultan necesarios e imprescindibles para la protección de los sistemas. Por otro lado, el derecho a la privacidad del individuo (entendida ésta como el control por parte de los individuos a determinar quién, cuándo, dónde y en qué condiciones puede ser accedida, procesada o transmitida información de carácter personal de un sujeto) está recogido en el marco legal vigente en Europa [21] y a nivel internacional[2].

La seguridad y la privacidad parecen disputar intereses opuestos, pero en las últimas décadas se han desarrollado mecanismos de privacidad responsable en los que los sujetos pueden operar con privacidad pero sin poder eludir las responsabilidades de sus acciones [22, 23, 24, 25, 26]. Algunos de estos mecanismos han sido desplegados en contextos

[2] http://www.ohchr.org/EN/UDHR

particulares para preservar aspectos concretos de privacidad, pero no ha sido posible integrarlos de manera apropiada y global en los sistemas actuales.

De entre las soluciones de privacidad responsable mencionadas, las credenciales o certificados anónimos son las que tienen mayor repercusión [27, 28, 29, 30, 31, 32, 33]. Con ellas se ha conseguido dotar de anonimato a credenciales digitales que certifican la identidad de un sujeto o cualquier otro atributo relacionado con el mismo. La semejanza con los esquemas de autenticación vigentes facilita su integración y despliegue en los sistemas existentes, además de que son compatibles con los marcos de actuación establecidos desde la seguridad de los sistemas de información.

Más formalmente, se definen las credenciales anónimas como aquellos certificados que dotan a un sujeto de una identidad digital compuesta por una serie de atributos relativos a su identidad real y que permite la acreditación parcial o total de los mismos, de forma anónima. La identidad real es considerada un atributo más. Algunas de las características más relevantes de este tipo de credenciales son:

- Permiten acreditar únicamente los atributos necesarios para el proceso de autenticación o autorización sin desvelar ninguna otra información. Esta acreditación no siempre conlleva la revelación del valor de estos atributos, permitiendo acreditar que los atributos toman valor dentro de un rango o pertenecen a un dominio establecido.
- Permiten establecer pruebas irrefutables de posesión de credenciales válidas sin tener que mostrar la credencial en sí.
- No son transferibles entre sujetos.
- Satisfacen la propiedad de no-enlazabilidad (varios usos de la misma credencial no pueden ser relacionados entre sí). Esta propiedad imposibilita la pérdida de privacidad que puede producirse al relacionar las distintas actividades de un mismo individuo dentro de la red.
- Por último, permiten la privacidad responsable, entendida como la posibilidad de gestión y depuración de responsabilidades pudiendo, bajo condiciones estrictas, la trazabilidad de una credencial hasta el sujeto real poseedor de la misma.

Sin embargo, a pesar de que las credenciales anónimas posibilitan el desarrollo de nuevos esquemas de autenticación digital basados en credenciales anónimas, el reto hoy en día, está en integrar este tipo de técnicas criptográficas a los servicios existentes y noveles de los sistemas de información, así como la implantación eficiente de los mismos. En el

contexto vehicular, existen propuestas que utilizan algunas de las citadas técnicas criptográficas para construir sistemas de peaje electrónico respetuosos con la privacidad de los participantes (e.g., [1]). Sin embargo, los autores no han encontrado ninguna propuesta que tenga por objetivo verificar telemáticamente las autorizaciones requeridas para circular de forma que se respete la privacidad de las entidades implicadas. La investigación llevada a cabo en el proyecto PRECIOUS ha tenido por objetivo contribuir a desarrollar un sistema de este tipo según los siguientes objetivos concretos:

1) Formalización de un modelo conceptual de las identidades digitales en el contexto de la circulación de vehículos.
2) Diseño de un sistema de la gestión de identidades digitales privado y responsable para el contexto de la circulación de vehículos. Aplicación al escenario de verificación automática y privada de las autorizaciones requeridas para circular.
3) Implementación de un demostrador del sistema.

## 3 RESOLUCIÓN

### 3.1 E-SAVE

#### 3.1.1 Modelo mejorado del proceso sancionador de infracciones administrativas para casos de exceso de velocidad

A partir de los resultados del proyecto VERA2, se ha desarrollado un modelo mejorado del proceso de infracciones administrativas para casos de exceso de velocidad [34]. El modelo desarrollado complementa el de VERA2 en cuanto que se identifican las entidades participantes tanto dentro como fuera del sistema (véase la Figura 1), las estructuras de datos y los intercambios de información realizados entre las entidades.

#### 3.1.2 Transmisión segura de información de avisos entre vehículos

Se propone un mecanismo basado en pruebas de esfuerzo (POW, del término en inglés Proof-Of-Work) y certificados electrónicos para dificultar la diseminación de mensajes de aviso falsos dentro de las VANETs (véase la Figura 2) [35]. La exigencia de presentar una prueba de esfuerzo para enviar un mensaje de aviso limita el número de mensajes de este tipo que un vehículo puede enviar y la utilización de certificados generados por el propio emisor permite obtener garantías de no repudio y por tanto permite trazar responsabilidades en su caso. Los análisis de rendimiento y seguridad realizados sobre el protocolo que se propone demuestran su robustez y viabilidad para ser desplegado en las VANETs.

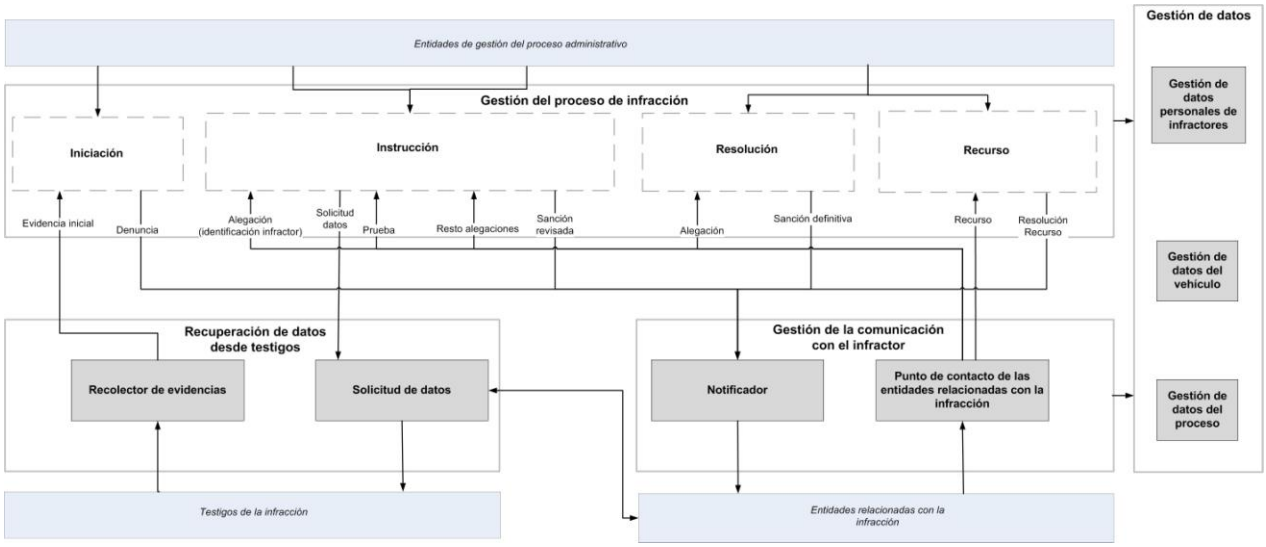
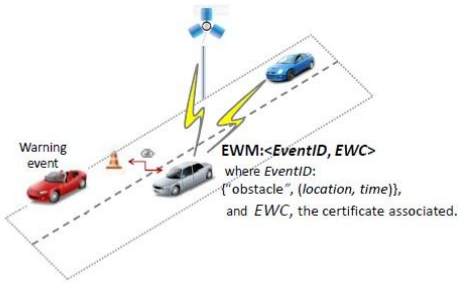



**Figura 1: Modelo del sistema propuesto para procesamiento sancionador de infracciones administrativas**




**Event Warning Certificate EWC**

| | |
|---|---|
| Certificate $C_e$: | |
| Serial-Number: | $I_e$ |
| Source: | $PKC_A$ |
| Message: | $h(EventID)$ |
| Movement: | $< pos, dir, vel >$ |
| POW: | $\mathcal{POW}(\omega, seed)$ |
| Validity Period: | $(ts_i, ts_f)$ |
| Crypto. Algorithms: | $Sign.Algorithm$ $Sign.Hash.Algorithm$ $m.Hash.Algorithm$ |
| Signature: | $s_A(C_e)$ |

**Figura 2: Representación gráfica del Certificado de Avisos que se propone, incluyendo la POW.**

### 3.1.3 Automatización del proceso de denuncias

Se propone la utilización de técnicas de esteganografía para embeber dentro de los mensajes de beacon la denuncia de comportamientos ilegales de vehículos circundantes evitando la posibilidad de ser detectados por los vehículos denunciados. La Figura 3 muestra el proceso de inserción de la denuncia (de momento solo la acción detectada e identificación del infractor) dentro de los mensajes de beacon. El proceso inverso de recuperación también ha sido definido. El análisis realizado demuestra que el sistema propuesto es viable computacionalmente teniendo en cuenta el estado actual de la tecnología vehicular y que existe al menos una posible configuración del sistema en la que éste es útil y operacional para los escenarios más comunes (autopistas, vías secundarias, vías urbanas).

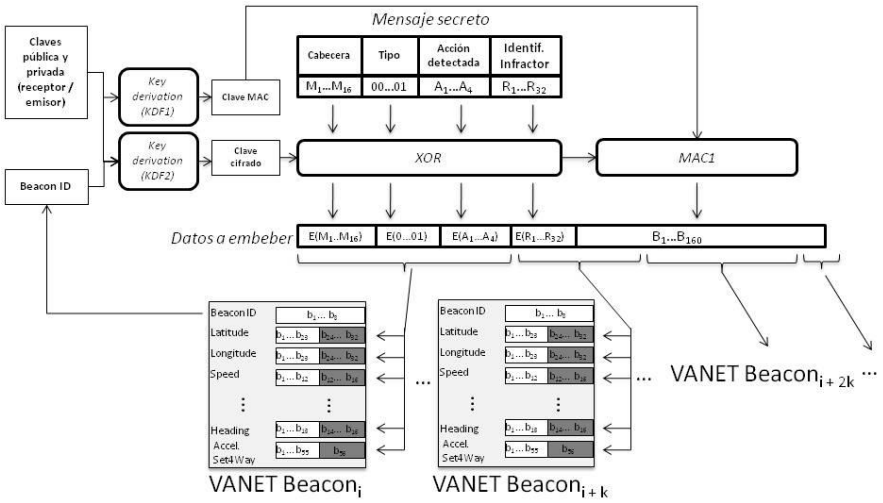



**Figura 3: Proceso de inserción de la denuncia dentro de los mensajes de beacon**

### 3.1.4 Automatización del proceso de notificaciones electrónicas para denuncias de tráfico

Se propone el diseño de un protocolo de intercambio de datos entre un vehículo y la infraestructura de comunicaciones para entregar notificaciones electrónicas de denuncias de tráfico con las garantías legales exigidas [36]. El análisis realizado sobre el protocolo arroja resultados satisfactorios en cuanto al cumplimiento de los requisitos legales y demuestra su viabilidad para implementarlo sobre plataformas comerciales.

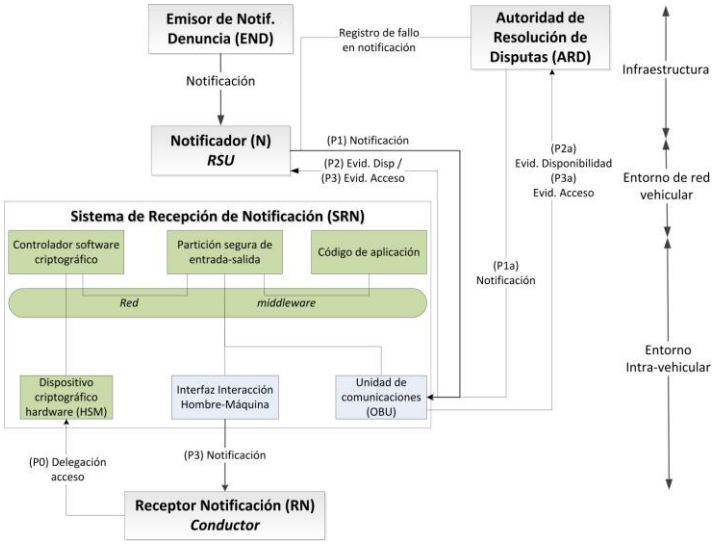



**Figura 4: Arquitectura de notificación con Tercera Parte Confiable**

### 3.1.5 Obtención de evidencias forenses vehiculares del comportamiento de un vehículo a partir de los vehículos colindantes

Se propone un protocolo que permite que un vehículo, tras recibir la notificación de una denuncia por infracción de tráfico, obtenga testimonios acerca del comportamiento del vehículo denunciado de los vehículos colindantes a éste en el momento de la detección de la infracción (véase Figura 5). Una vez recolectadas las evidencias disponibles, se envían a la Autoridad para su evaluación. Los resultados de simulación del protocolo muestran que para un intervalo de 5 segundos, (1) en entornos urbanos se puede contactar con el 90% de los testigos, y (2) en autopistas se puede conseguir un máximo de 38 testimonios en media.

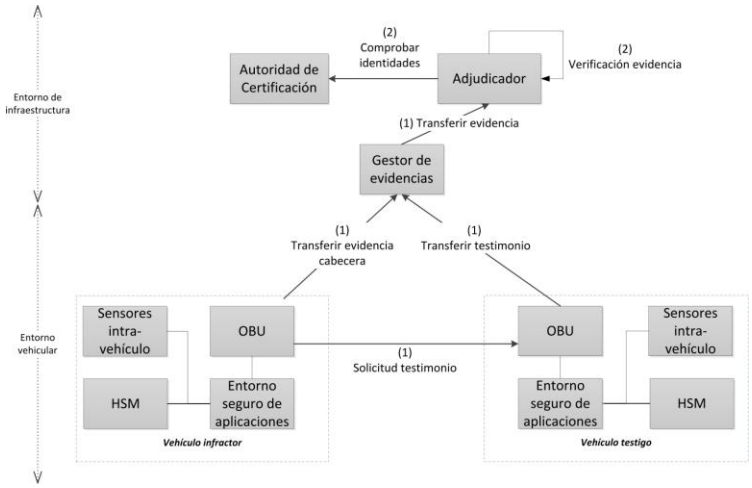



**Figura 5: Arquitectura del sistema propuesto para la obtención de evidencias sobre el comportamiento de un vehículo a partir de los vehículos colindantes**

## 3.2 PRECIOUS

### 3.2.1 Modelo mejorado de las credenciales necesarias para circular

Para poder construir un sistema de credenciales electrónicas, es necesario contar primero con un modelo claro de dichas credenciales. Así que en primer lugar se analizó la legislación pertinente española y, a partir de ahí, se elaboró un modelo de las actuales credenciales requeridas para circular [37]. La Figura 6 refleja dicho modelo de datos utilizando UML.

En la Figura 7 se presenta en modelo de datos que se propone para las credenciales requeridas para circular que mejora al actual al eliminar los atributos redundantes, y las relaciones y credenciales innecesarias.

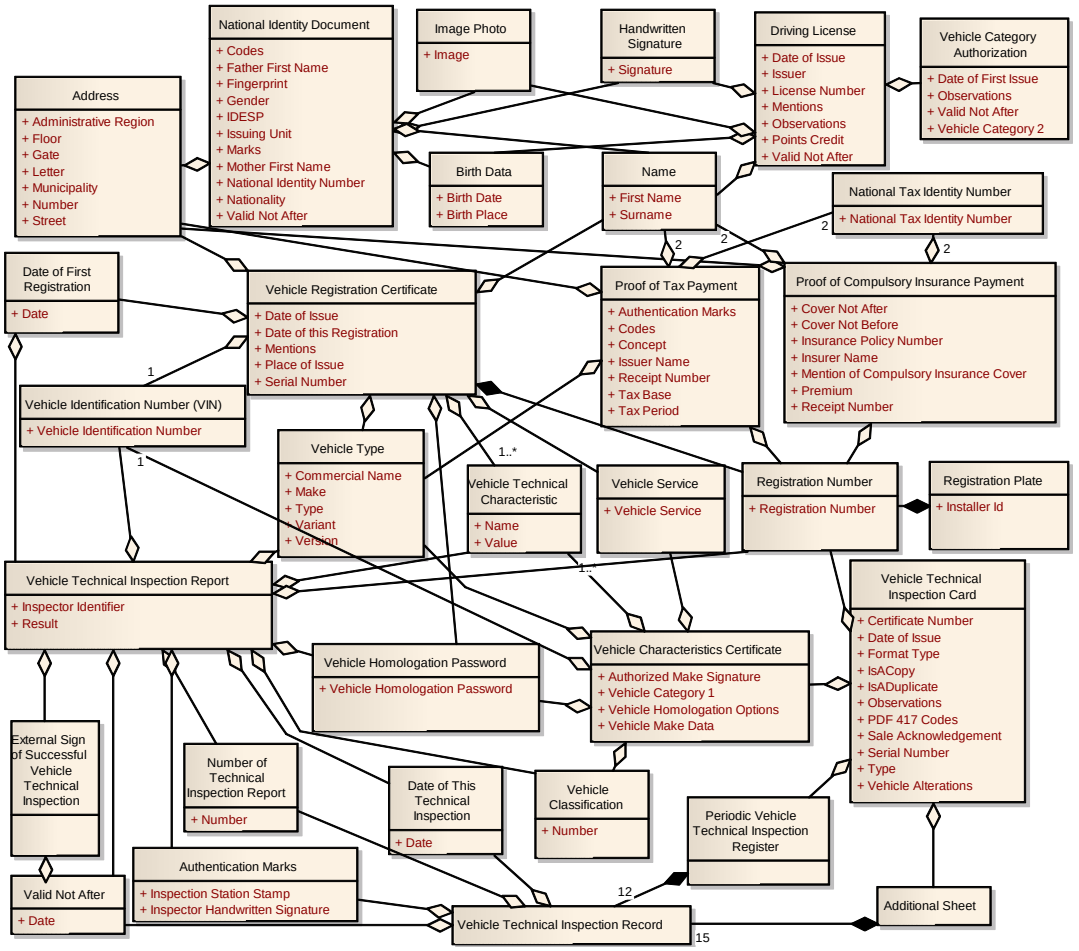



**Figura 6: Modelo de datos de las credenciales requeridas para circular en el momento actual (según la legislación española)**

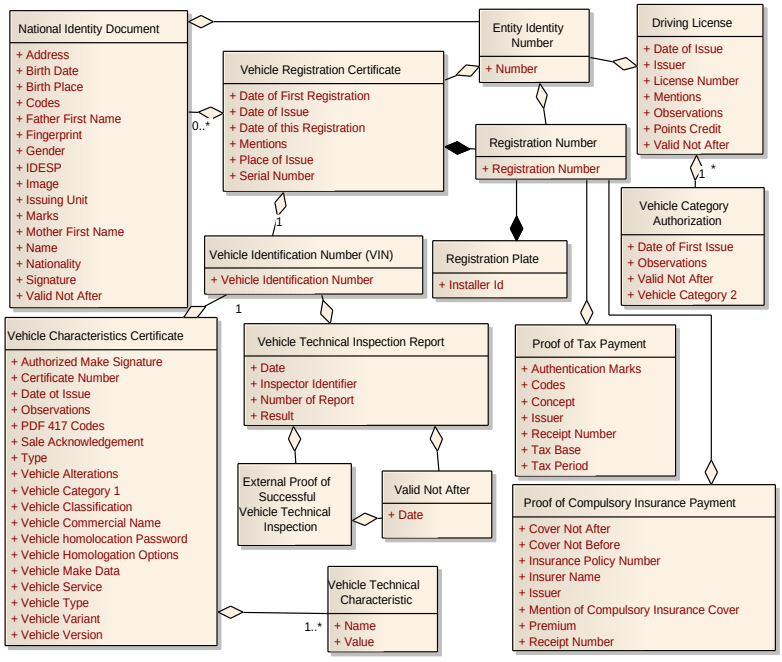



**Figura 7: Modelo de datos de las credenciales para circular que se propone**

### 3.2.2 Análisis comparativo de los sistemas de credenciales anónimas

En paralelo, se analizaron los sistemas de credenciales anónimas más relevantes para estudiar su idoneidad como fundamento del sistema de verificación de las autorizaciones requeridas para circular objeto de este proyecto [37]. El resumen del análisis se muestra en la Tabla 1.

**Tabla 1: Análisis comparativo de las propiedades principales de los sistemas de credenciales anónimos estudiados. Se asume que un usuario está asociado a β atributos y que desea realizar α procesos de verificación no enlazables, donde cada proceso de verificación se repite δ veces.**

| | Brands [2] | Kwon [4] | Chameleon [5] | Camenish [3] | Verheul [6] |
|---|---|---|---|---|---|
| No. of Certificates | $\alpha\delta$ | $\alpha\delta$ | 1 | $\alpha$ | $\alpha$ |
| Workload | $O(\beta)$ | $O(\beta)$ | $O(\beta)$ | $O(\beta)$ | $O(\beta)$ |
| Accept Non Predefined Control Policies? | ✓ | ✓ | ✓ | × | × |
| Commercial Implementation | U-prove | × | × | Idemix | × |
| Unlinkability (Pseudonyms Changes) | × | × | × | × | |
| PKI Standard Compliance | × | ✓ | ✓ | × | × |
| Anonymous Credential Acquirance | ✓ | ✓ | ✓ | ✓ | ✓ |

### 3.2.3 Diseño de un sistema de credenciales anónimas para entornos vehiculares

Por su eficiencia, flexibilidad y escalabilidad se ha elegido el sistema de Persiano et al. [30] como base para proponer un sistema de credenciales anónimas adaptado para la verificación automática y privada de las autorizaciones requeridas para circular. El sistema inicial ha sido modificado y extendido para satisfacer dos aspectos fundamentales:

- Permitir la validación conjunta del mismo atributo contenido en dos credenciales diferentes pero poseídas por un mismo usuario.
- Permitir pruebas no-interactivas. Se han minimizado al máximo las interacciones entre probador y verificador.

Se han desarrollado un nuevo algoritmo de generación de compromisos y cuatro nuevos algoritmos de prueba no interactiva de conocimiento nulo (NI ZK-PoK):

- NI ZK-PoK-1 de la composición booleana de una representación RSA.
- NI ZK-PoK-2 de una representación del logaritmo discreto.
- NI ZK-PoK-3 del logaritmo discreto de una parte de una representación del logaritmo discreto.
- NI ZK-PoK-4 de la raíz e-ésima de una parte de una representación del logaritmo discreto.

El resumen del coste computacional del sistema de credenciales propuesto se muestra en las Tablas 2 y 3.

**Tabla 2: Número de veces que se ejecuta cada una de las pruebas de conocimiento nulo durante la fase de prueba conjunta de dos credenciales anónimas y número de secretos requeridos en cada prueba de conocimiento.**

| Operational Cost | | | |
|---|---|---|---|
| | Operation | Quantity | Number of secrets $n$ |
| ZK-POK-1 | Non-interactive ZK-PoK of a boolean composition of RSA-representations | 1 | n=4 |
| ZK-POK-2 | Non-interactive ZK-PoK of a DL-representation | 2 | n=4 |
| ZK-POK-3 | Non-interactive ZK-PoK the DL of part of a DL-representation | 2 | n=l |
| ZK-POK-4 | Non-interactive ZK-PoK of the e-th root of part of a DL-representation | 2 | n=2 |

**Tabla 3: Coste computacional del sistema en función del número de exponenciaciones modulares en cada fase. Po indica que se calcula una vez, Pre indica pre-calculado y Run indica que se calcula mientras se ejecuta el protocolo.**

| Number of modular exponentiations in each phase | | |
|---|---|---|
| | Organization | |
| Setup | 3 ($Po$) | |
| Anonymous Credential Issuing | 4 ($Po$) | |
| | Prover | Verifier |
| Anonymous Credential Joint Proving | | |
| Construct Commitments | 6 ($Po$) + 14 ($Pre$) + 0 ($Run$) | — |
| ZK-POK-1 | 17 ($Pre$) | 17 ($Run$) |
| ZK-POK-2 | 8 ($Pre$, n=4) | 10 ($Run$, n=4) |
| ZK-POK-3 | 2·l ($Pre$) | 2·l ($Run$) |
| ZK-POK-4 | 3 ($Pre$) | 3 or 4 ($Run$) |

### 3.2.4 Diseño del sistema de verificación automática de las autorizaciones requeridas para circular

Se ha diseñado un sistema de verificación automática y privada de las autorizaciones requeridas para circular que se construye sobre el sistema de credenciales descrito anteriormente. La arquitectura general del sistema se muestra en la Figura 8.

Las credenciales de los conductores y vehículos se dividen en dos conjuntos diferenciados:

1) Las credenciales básicas, equivalentes directos y en formato electrónico tradicional (X.509, firma digital) de las actuales credenciales según el modelo de credenciales propuesto. Estas credenciales se muestran en la Figura 9, así como su tipo (X.509 PKC, X.509 ATC, firma digital, WAVE PKC). Los emisores de estas credenciales son los mismos que en la actualidad (Autoridad de Tráfico, Ministerio de Industria, fabricantes de los vehículos…).

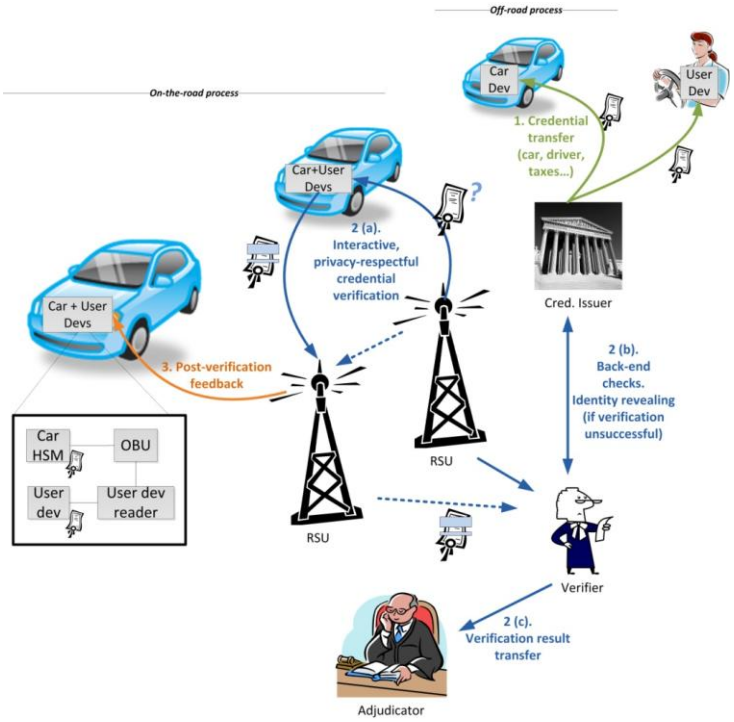



**Figura 8: Arquitectura a alto nivel del sistema**

2) Las credenciales anónimas, que siguen el sistema de credenciales de Persiano et al. modificado y extendido. Estas credenciales se emiten por una autoridad específica y contienen los atributos de su equivalente básico que se muestran en la Figura 9. Nótese que se establecen como privados los atributos que suponen una identificación directa del vehículo o del conductor (VIN, número de matrícula, identificación asociada al DNIe), y públicos los otros atributos como son los periodos de validez o los distintos tipos de vehículos considerados.

Se asume que tanto el conductor como el vehículo cuentan con un dispositivo seguro para alojar las credenciales y los programas que las manejan. En el caso del vehículo este dispositivo (CarDev) se corresponde con el HSM (Hardware Security Module) alojado en la OBU (On-Board Unit). En el caso del conductor (UserDev) se asume un único dispositivo similar al actual DNIe que aloja, además de esta credencial, un permiso de conducir electrónico. Se asume que el vehículo cuenta con un mecanismo seguro de comunicación con el dispositivo de credenciales del conductor. Ambos dispositivos deben contar con espacio suficiente para contener los dos conjuntos de credenciales de cada entidad y la capacidad suficiente para utilizarlas.

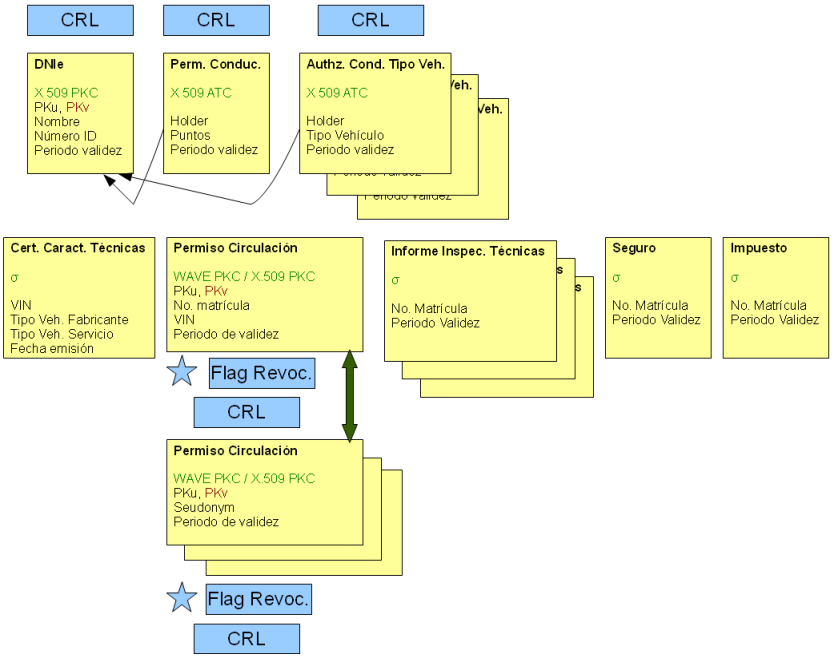



**Figura 9: Representación del conjunto de credenciales básicas, su tipo y los atributos de éstas que deben ser incluidos en las credenciales anónimas. Nótese que las credenciales seudónimos del permiso de circulación se muestran por completitud, ya que no tienen equivalente en el conjunto de credenciales anónimas propuesto.**

Se asume que la entidad que gestiona el sistema verificador es distinta a la Autoridad de Tráfico. El sistema verificador está desplegado en un conjunto de RSUs (Road Side Units), que alojan los agentes verificadores. Los agentes verificadores interpelarán a los vehículos telemáticamente para verificar las autorizaciones requeridas para conducir. Los agentes verificadores se complementan con cámaras fotográficas que se utilizan en el caso de que la verificación telemática falle. Nótese que el vehículo actúa como intermediario entre el sistema de verificación y el dispositivo del conductor. En cualquier caso, se informa al par vehículo/conductor del resultado de la verificación telemática.

Una vez se ha inicializado el sistema de credenciales y se han emitido las credenciales del conductor y del vehículo, las fases del protocolo son las siguientes:

1) Pre-cálculo de las NI ZK-PoK por parte de los dispositivos del conductor y del vehículo UserDev y CarDev.
2) Arranque del vehículo. El conductor enlaza su UserDev con el CarDev utilizando el mecanismo de comunicación disponible. Tras autenticarse el conductor como el poseedor legítimo del UserDev (y por tanto de las credenciales que aloja), UserDev envía a CarDev el permiso de conducir que contiene y prueba la posesión de la clave privada del mismo a éste.

3) Interpelación por parte de un Agente Verificador al par vehículo/conductor para que se demuestre posesión de las autorizaciones requeridas para circular.
4) El UserDev envía al Agente Verificador a través del CarDev las NI ZK-PoK correspondientes al permiso de conducción (1 NI ZK-PoK-2, 1 NI ZK-PoK-3 y 1 NI ZK-PoK-4) y a las autorizaciones para conducir determinado tipo de vehículos (por cada autorización existente, 1 NI ZK-PoK-1, 2 NI ZK-PoK-2, 2 NI ZK-PoK-3 y 2 NI ZK-PoK-4).
5) El CarDev envía al Agente Verificador las NI ZK-PoK correspondientes al permiso de circulación (1 NI ZK-PoK-2, 1 NI ZK-PoK-3 y 1 NI ZK-PoK-4) y al resto de credenciales necesarias para circular (por cada una de las cuatro credenciales adicionales, 1 NI ZK-PoK-1, 2 NI ZK-PoK-2, 2 NI ZK-PoK-3 y 2 NI ZK-PoK-4).
6) El Agente Verificador verifica las pruebas de conocimiento nulo enviadas.

En caso de verificación positiva (todo es correcto)

7) El Agente Verificador informa al par vehículo/conductor.

En caso de verificación negativa (alguna de las pruebas ha fallado),

8) El Agente Verificador ordena la realización de una foto del vehículo.
9) El Agente Verificador informa al CarDev del resultado fallido y solicita al CarDev la identificación del conductor.
10) El CarDev envía al Agente Verificador el permiso de conducción del conductor.
11) El Agente Verificador envía a la Autoridad de Tráfico las evidencias recolectadas.

Las credenciales anónimas no son revocables, pero sí lo son algunas de las credenciales básicas. Este tema se ha solventado asumiendo que se puede hacer llegar de forma segura al CarDev, y con cierta frecuencia (e.g., cuando el vehículo reposte o sea aparcado), información acerca de qué credenciales han sido revocadas (tanto aquellas correspondientes al propio vehículo como aquellas correspondientes al conjunto de sus conductores habituales). En caso de que alguna credencial esté revocada, el propio CarDev (más concretamente su parte confiable, el HSM) así lo indicará al Agente Verificador, resultando en una verificación negativa.

Los resultados preliminares del análisis de viabilidad realizado sobre el rendimiento del protocolo son satisfactorios aunque es necesario confirmarlos aún.

## 4 CONCLUSIONES

En general se puede decir que los resultados de ambos proyectos reflejan que sería viable introducir las tecnologías ITS y las VANETs en el contexto vehicular para mejorar la supervisión y la gestión de ciertas normas de tráfico. Se prevé en el caso de que así se hiciera un impacto altamente beneficioso en la seguridad vial. Aunque ambos proyectos han abordado teóricamente y a través de simulaciones casi todos sus objetivos, queda aún pendiente en ambos la implementación e integración de las propuestas en sistemas reales. Esta es la principal línea futura de trabajo para ambos proyectos, en el desarrollo de la cual sería deseable contar con la colaboración de empresas del sector y de los organismos públicos implicados.

## AGRADECIMIENTO

Este trabajo ha sido realizado en el marco del proyecto E-SAVE, subvencionado por el Ministerio de Ciencia e Innovación (referencia TIN2009-13461) y del proyecto PRECIOUS, subvencionado por la Comunidad de Madrid (referencia CCG10-UC3M/TIC-5174).

## BIBLIOGRAFÍA

1. TRONCOSO, C, ET AL (2007). “PriPAYD: Privacy friendly Pay-As-You-Drive insurance”. Alexandria, Virginia, USA: ACM WPES'07. pp. 99-107.

2. GIBSON, C.H. (1997) “Automated Highway Merging Protocols and their effectiveness on highway operations and vehicle performance”.

3. ESPAÑA (2008) “Proyecto de Ley 121/000012”. Boletín Oficial de las Cortes Generales. Madrid : s.n., pp. 1-21.

4. DIRECCIÓN GENERAL DE TRÁFICO (2008). “Nota de prensa. Nuevo sistema para tramitación de denuncias”. Madrid : s.n.

5. GUETTE, G. AND BRYCE, C. (2008) “Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)”. International Federation for Information Processing. WISTP 2008. pp. 106-116.

6. RAYA M., PAPADIMITRATOS P. AND HUBAUX, J.P. (2006) “Securing vehicular communications”. IEEE Wireless Communications, pp. 8-15.

7. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) (2007). “ISO 24535:2007 Intelligent transport systems -- Automatic vehicle identification -- Basic electronic registration identification (Basic ERI)”.

8. NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION. DEPARTMENT OF TRANSPORTATION (2006). “Event Data Recorders”. Washington (Estados Unidos).

9. WOLF M., WEIMERSKIRCH A. AND PAAR C (2004). “Security in automotive bus systems”. Embedded Security in CARs (ESCAR).

10. SOCIETY OF AUTOMOTIVE ENGINEERS (2008). “SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary”.

11. EUROPEAN COMMISSION (2010) “Road safety programme 2011-2020: detailed measures. Tech. Rep. MEMO/10/343”.

12. NATIONAL ASSOCIATION OF BREAKDOWN SERVICE BUSINESSES (ANEAC) (2010). “Driving without having passed the technical inspection will not cause the immediate removal of its credential”. URL http://www.aneac.com/index.php/2010/04/la-caducidad-de-la-itv-no-sera-motivo-para-quitar-el-carne/

13. S.P.A, A. (2011). “More than 1 million vehicles without insurance policy”. URL http://www.seguros.es/noticias/mas-de-un-millon-de-coches-sin-seguro.html

14. AUTOCAR (2008). “Untaxed vehicles on the rise”. URL: http://www.autocar.co.uk/News/NewsArticle/AllCars/232243/

15. DEPARTMENT FOR TRANSPORT, U.K.(2004) “Project: Unlicensed drivers”. URL http://www.dft.gov.uk/rmd/project.asp?intProjectID=10120

16. EUROPEAN COMMISSION (2004). “Commission directive 2003/127/ec of 23 december 2003 amending council directive 1999/37/ec on the registration documents for vehicles”. In: Official Journal of the European Union, vol. 10, pp. 29-53.

17. EUROPEAN COMMISSION (2006) “Directive 2006/126/ec of the european parliament and of the council of 20 december 2006 on driving licences”. In: Official Journal of the European Union, vol. 403, pp. 18-60.

18. EUROPEAN COMMISSION (2007). “Directive 2007/46/ec of 5 september 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles”. In: Official Journal of the European Union, vol. 263, pp. 1-160.
(2007)

19 TISPOL. “Identifying and fining the owner of the vehicle”. URL: https://cleopatra.tispol.org/cleopatra/europe/general/technology/identifying-and-fining-owner-vehicle/identifying-and-fining-owne

20 ESPAÑA (2006). “Orden itc/2536/2006, de 26 de julio, por la que se regula el soporte electrónico para la tarjeta itv y se modifican los anexos 10 y 11 del real decreto 2140/1985, de 9 de octubre, por el que se dictan normas sobre homologación de tipos de vehículos, remolques, semirremolques, así como de partes y piezas de dichos vehículos”. In: Boletín Oficial del Estado, vol. 184, pp. 28.994-28.994.

21 EUROPEAN COMMISSION (1995). “Directiva Europea 95/46/EC, “Protection of individuals with regard to the processing of personal data and on the free movement of such data”.

22 A. LYSYANSKAYA, R. RIVEST, A. SAHAI, S. WOLF (2000), “Pseudonym systems,” Proc. Selected Areas in Cryptography, SAC’99.

23 D. CHAUM, E. VAN HEYST (1991), “Group signatures,” in Eurocrypt’91.

24 D.CHAUM (1983). “Blind signatures for untraceable payments,” in Advances in Cryptology (Crypto’82).

25 A. SHAMIR (1985). “Identity-based cryptosystems and signature schemes,” Advances in Cryptology.

26 D. BONEH AND M. FRANKLIN (2001), “Identity-based encryption from the weil pairing,” Advances in Cryptology (CRYPTO’01).

27 S. BRANDS (2000). Rethinking Public-Key Infrastructures and Digital Certificates: Building in Privacy, MIT Press.

28 J. CAMENISCH, A. LYSYANSKAYA (2001), "An Efficient System for Non-Transferable Anonymous Credentials," Proc. Eurocrypt 2001.

29 J. CAMENISCH, A. LYSYANSKAYA (2002), "A Signature Scheme with Efficient Protocols," Proc. Security in Communication Networks.

30 P. PERSIANO, I. VISCONTI (2003), “An anonymous credential system and a privacy-aware PKI,” Proc. Australasian conference on information security and privacy (ACISP).

31 R. GANGISHETTI, M. C. GORANTLA, M. L. DAS, A. SAXENA (2006), “Identity based multisignatures,” Informatica, vol. 17, no. 2.

32 J. GROTH, A. SAHAI (2008), “Efficient non-interactive proof systems for bilinear groups,” in EUROCRYPT 2008.

33 M. BELENKIY, J. CAMENISCH, M. CHASE, M. KOHLWEISS, A. LYSYANSKAYA, H.SHACHAM (2009). “Randomizable proofs and delegatable anonymous credentials,” Advances in Cryptology (CRYPTO 2009).

34 J. M. DE FUENTES, A.I. GONZÁLEZ-TABLAS, J. L. HERNÁNDEZ-ARDIETA, A. RIBAGORDA. “Towards an automatic enforcement for speeding: enhanced model and ITS realization”, IET Intelligent Transport Systems. (En revisión con cambios menores)

35 E. PALOMAR, J. M. DE FUENTES, A. I. GONZÁLEZ-TABLAS, A. ALCAIDE (2011). Hindering false event dissemination in VANETs with proof-of-work mechanisms, Transportation Research Part C: Emerging Technologies, Available online 4 November 2011, ISSN 0968-090X, 10.1016/j.trc.2011.08.002. (http://www.sciencedirect.com/science/article/pii/S0968090X11001124)

36. J. M. DE FUENTES, A. I. GONZÁLEZ-TABLAS, L. GONZÁLEZ-MANZANO, A. RIBAGORDA (2012). “Diseño de un protocolo para el envío de notificaciones de denuncias por hechos de circulación al vehículo a través de tecnologías ITS”. XII Congreso Español de ITS, Madrid 2012.

37. A.I. GONZÁLEZ-TABLAS, A. ALCAIDE, G. SUAREZ-TANGIL, J.M. DE FUENTES, I. BARROSO-PEREZ (2011). “Towards a privacy-respectful telematic verification system for vehicle & driver authorizations (poster)”. Eighth Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2011), Copenhagen (Denmark), LNICST, Springer, ISBN pending, pp. pending, 4 pages.