RESPUESTA A LAS PREGUNTAS HECHAS POR: JOSE VICENTE PERALTA ROMERO, EN RADICADO NO. 2012-321-024995-2 Y POR CAMILO A. RUBIO, EN RADICADO NO. 2012-321-023760-2

TECNOLOGÍA Y RENDIMIENTO

P/. ¿Cuál es el propósito original de la tecnología propuesta por este decreto?

R/. La tecnología especificada fue diseñada para identificación por radio frecuencia en aplicaciones de logística soportando lecturas a alta velocidad.

P/. ¿Qué estadísticas exactas de eficiencia del cobro de peajes, avaladas por una entidad independiente y sin considerar la aplicación de tecnologías o dispositivos de apoyo (redundantes), pueden ser proporcionadas para esta tecnología exactamente de acuerdo a la versión del estándar mencionado en el decreto ministerial?

R/. En Marzo de 2011, la State Road and Tollway Authority de Georgia junto con Georgia DOT (Department of Transportation) avalan las pruebas de lectura realizadas con la tecnología ISO 18000 6c a velocidades superiores a 85mph con resultados de confiabilidad de lectura del 100%.

PRESENCIA EN EL MERCADO INTERNACIONAL (REFERENCIAS Y EXPERIENCIAS DE PROYECTOS A NIVEL MUNDIAL)

P/. ¿En qué países se ha adoptado esta tecnología, exactamente de acuerdo a la versión del estándar mencionado en el decreto ministerial, de forma exitosa para su aplicación simultánea y paralela en identificación vehicular y recaudo electrónico de peajes a través de un dispositivo único?

R/. En México se implementó el sistema REPUVE que permite la identificación electrónica vehicular a nivel nacional basado en la tecnología ISO 18000–6C. Actualmente se encuentran en implementación tanto los dispositivos a bordo como la infraestructura de carretera. Por otro lado, Caminos y Puentes Federales de Ingresos y Servicios Conexos ("CAPUFE"), la autoridad de peajes de México instaló con éxito líneas de peaje con la tecnología mencionada y que se encuentran integrados con el REPUVE.

Adicionalmente, en países asiáticos y europeos como Tailandia, Taiwán y Turquía se ha también implementado la tecnología ISO 18000-6c para aplicaciones de identificación electrónica vehicular.

Existen otros proyectos en implementación a nivel latinoamericano como son el caso de Perú que ha implementado stickers en los vehículos del país, y Brasil donde se encuentra en implementación el sistema SINIAV para identificación electrónica vehicular basada en modificaciones del estándar ISO 18000-6C que será también utilizado en el recaudo de peajes.

P/. ¿Qué referencias existen para la utilización de la tecnología sugerida, exactamente de acuerdo a la versión del estándar mencionado en el decreto ministerial, para el recaudo electrónico de peajes en entornos "multi-lane free flow"?

R/. Entre otros se pueden mencionar los casos de:

- Washington State Department of Transportation, WA,
- E-470 Public Highway Authority, CO
- State Road Tolling Authority, Georgia
- SR-91 Express Lanes, Orange County, CA
- Texas Department of Transportation (SH130, SH45)
- Port Mann Bridge, Vancouver, British Columbia, Canada

P/. ¿Qué referencias existen para la utilización de esta tecnología, exactamente de acuerdo a la versión del estándar mencionado en el decreto ministerial, en esquemas de cargo por congestión, como el recientemente anunciado por la ciudad de Bogotá?

R/. No existen actualmente esquemas de cargos por congestión con el estándar mencionado. A nivel mundial, existen pocos casos documentados de esquemas de cargos por congestión (Londres, Milán, Singapur siendo los más conocidos) cuya aplicación se da por cámaras, tags activos, semi-activos y pasivos por lo que no se puede hablar de un estándar a nivel mundial para la aplicación de cargos por congestión.

P/. ¿La tecnología mencionada permite el uso de aplicaciones locales en el dispositivo (autónomas), que permitan el intercambio de información con infraestructura localizada en sitios que presentan dificultades para la red de comunicación (por ejemplo en sitios remotos en el caso de interrupciones de las redes de comunicación).

R/. La arquitectura propuesta no hace uso de aplicaciones locales en el dispositivo (autónomas) y se basa en la identificación de los vehículos mediante su dispositivo a bordo lo que no depende de las redes de comunicación. La arquitectura propuesta permite la existencia de puntos de lectura tanto en línea como fuera de línea.

PROVEEDORES Y FABRICANTES.

P/. ¿Cuál es la cobertura de la tecnología sugerida en cuanto a la cantidad de antenas lectoras y cantidad de dispositivos a nivel mundial, exactamente de acuerdo a la versión del estándar mencionado en el decreto ministerial?

R/. De acuerdo con los proveedores, actualmente existen más de 30 millones de dispositivos ISO 18000-6c instalados a nivel mundial.

P/. ¿De qué manera se pretende garantizar la existencia de un mercado abierto con la participación de múltiples proveedores y fabricantes.

R/. Al tratarse de un estándar abierto definido por la International Standards Organisation (ISO), se asegura la existencia de un mercado abierto con la participación de múltiples proveedores y fabricantes.

P/. ¿Cuántas empresas en el mundo pueden demostrar referencias para proveer la tecnología mencionada, exactamente de acuerdo a la versión del estándar mencionado en el decreto ministerial?

R/. En este momento existe información sobre 3 proveedores de la tecnología ISO 18000 6c.

P/. ¿Qué ejemplos de interoperabilidad entre diferentes fabricantes existen para la tecnología mencionada, exactamente de acuerdo a la versión del estándar mencionado en el decreto ministerial?

R/. México es un ejemplo de interoperabilidad técnica donde para el REPUVE proveedores diferentes proveen los dispositivos a bordo y las antenas lectoras.

TECNOLOGÍA

P/. ¿Cuál es el tiempo promedio de vida de los dispositivos de la tecnología 18000-6c?

R/. Los fabricantes garantizan que los dispositivos a bordo pueden llevar a cabo más de 100 000 ciclos de lectura/escritura.

P/. ¿La utilización de esta tecnología implica el uso de patentes por parte de un proveedor para su aplicación en esquemas de peaje electrónico?

R/. La arquitectura propuesta no requiere el uso de patentes por parte de proveedor alguno para la aplicación de peaje electrónico.

P/. ¿La tecnología mencionada permite algún medio de retroalimentación o comunicación directa con el usuario en tiempo real?

R/. La arquitectura propuesta no contempla retroalimentación con el usuario en tiempo real a través del OBU, lo que no implica que no se podrán utilizar otros medios de retroalimentación en tiempo real como lo son internet o mensajes de texto a través de celular.

CONFORMIDAD DEL ESTÁNDAR

P/. ¿El dispositivo estipulado debe estar configurado exactamente según la norma 18000-6c?

R/. El dispositivo estipulado debe estar configurado exactamente según la última actualización de la norma ISO 18000-6.

P/. ¿Es un requerimiento la adquisición de dispositivos norma 18000-6c 2006 por parte de fabricantes independientes?

R/. El Decreto no establece los requerimientos de participación de fabricantes para efectos de provisión de los dispositivos de a bordo ni de ningún otro dispositivo para el Ministerio de Transporte.

P/. ¿El Ministerio de Transporte aceptará como proveedores de tecnología a fabricantes de equipos utilizando protocolos propietarios, producto de una modificación del estándar 18000-6c-2006 y por definición incompatibles con el mismo?

R/. El Decreto no establece los requerimientos de participación de fabricantes para efectos de provisión de los dispositivos de a bordo ni de ningún otro dispositivo para el Ministerio de Transporte.

SEGURIDAD

P/. ¿Existe en el estándar ISO 18000-6c – 2006 alguna definición respecto de la seguridad bancaria?

R/. El estándar no hace definiciones al respecto de la seguridad bancaria. Las transacciones dentro de la arquitectura propuesta entre el dispositivo a bordo y la antena lectora no son en ningún caso transacciones bancarias y por lo tanto la comunicación no contempla este tipo de estándares de seguridad bancaria. En el caso de llevarse a cabo alguna transacción bancaria se llevará a cabo en el back-office, por lo que no se requiere ningún tipo de especificación dentro de la tecnología que deba tenerse en cuenta para implementar seguridad bancaria.

P/. ¿Cuáles son los mecanismos de seguridad implementados en el dispositivo de acuerdo al estándar mencionado en el decreto?

R/. Los mecanismos de seguridad implementados en el dispositivo de acuerdo al estándar mencionado son:

- Password estático de 32 bits
- Comando de "kill" o autodestrucción
- CRC de 16-bits
- PRNG de 16-bits

P/. ¿El estándar ISO 18000-6c provee una especificación clara para completar una transacción monetaria, incluyendo algoritmos de seguridad no propietarios a fin de permitir la interoperabilidad y la posibilidad de un mercado con múltiples operadores?

R/. Como se aclaró en una pregunta anterior, la arquitectura propuesta lleva a cabo las transacciones bancarias en el back-office, en caso de llevarse a cabo, por lo que no se requiere ningún tipo de especificación dentro de la tecnología para completar transacciones monetarias.

P/. ¿Existe una protección de lectura en la norma ISO 18000-6c 2006 para asegurar la confidencialidad?

R/. La norma ISO 18000-6c cuenta con un password estático de 32 bits para proteger contra lectura.

P/. ¿De qué manera es posible proteger la lectura del TID de un dispositivo fabricado según la norma ISO 18000-6c por medio de una antena lectora RFID común?

R/. De acuerdo a la norma ISO 18000-6c, es posible implementar un mecanismo de autenticación de antenas lectoras basado en un esquema de pregunta-respuesta entre antena y lector de manera que sólo antenas lectoras auténticas puedan leer los TID de los dispositivos.

P/. ¿De qué manera se puede asegurar que no exista la posibilidad de emular o clonar el TID de un dispositivo fabricado según la norma ISO 18000-6c-2006?

R/. Con suficiente tiempo y recursos cualquier tecnología de identificación podrá ser clonada o emulada. No es entonces posible asegurar ninguna tecnología contra estos ataques.

Todos los dispositivos que cumplen con el estándar ISO 18000-6c cuentan con un número único de identificación que viene pregrabado de fábrica y no puede ser modificado. El estándar ISO 18000-6c establece la numeración asignada a cada uno de los fabricantes de chips en el mundo, lo cual garantiza que no habrá TIDs iguales entre diferentes fabricantes. La clonación de dispositivos implicaría contar con una fábrica pirata de semiconductores, lo cual es altamente improbable y prohibitivo en términos de costos.

En cuanto a la emulación, se requeriría un proceso doble de: 1. Escucha de las conversaciones entre tags y antenas y 2. El proceso de emulación. Los equipos necesarios para estos procesos no se encuentran disponibles fácilmente en el mercado y sus costos serían prohibitivos debido al desarrollo y tiempo requeridos.

Aparte de esto, el dispositivo a bordo deberá contará con mecanismos visuales de seguridad y será plenamente visible por cualquier autoridad, de tal forma que si es emulado será evidente que un vehículo no cuenta con el dispositivo.

P/. ¿Cuáles son las consecuencias para el sistema si el TID de un dispositivo fabricado según la norma ISO 18000-6c 2006 es emulado o clonado?

R/. Para cualquier tecnología, en caso de clonación o emulación de una unidad a bordo junto con la falsificación de la placa física, implicaría que un vehículo podría hacerse pasar por otro.

P/. ¿Qué mecanismos de seguridad están implementados en la comunicación entre antena y dispositivo para detectar posibles dispositivos clonados?

R/. Ninguna tecnología puede detectar durante la transacción un dispositivo perfectamente clonado. Los mecanismos para controlar este tipo de eventos siempre se deben implementar en el back-office. El proyecto de decreto prevé que el Ministerio de Transporte podrá definir en una siguiente etapa, y basándose en un análisis de conveniencia, la implementación de un esquema de seguridad de su propiedad encima del protocolo definido, que tendrá que ser de

obligatorio cumplimiento por todos los proveedores de la tecnología para asegurar una verificación de la autenticidad de los dispositivos.

P/. ¿Es posible para una antena lectora RFID verificar la autenticidad de un dispositivo fabricado según la norma ISO 18000-6c -2006 en tiempo real?

R/. La norma 18000-6c no contempla mecanismos de verificación de autenticidad de dispositivos. El proyecto de decreto prevé que el Ministerio de Transporte podrá definir en una siguiente etapa, y basándose en un análisis de conveniencia, la implementación de un esquema de seguridad de su propiedad encima del protocolo definido, que tendrá que ser de obligatorio cumplimiento por todos los proveedores de la tecnología para asegurar una verificación de la autenticidad de los dispositivos.

P/. ¿De qué manera está implementada la escritura de datos en un dispositivo fabricado según la norma ISO 18000-6c 2006?

R/. Para entender cómo se encuentra implementada la escritura en dispositivos, por favor referirse a la norma ISO 18000-6c 2006. La arquitectura propuesta no almacenará ningún tipo de información en el dispositivo por lo que la escritura de datos no es relevante dentro de la arquitectura.

P/. ¿De qué manera está regulado el acceso a los datos de un dispositivo fabricado según la norma ISO 18000-6c?

R/. La arquitectura propuesta no almacenará ningún tipo de información en el dispositivo, por lo que no es necesario regular el acceso a los datos.

P/. ¿Existe la posibilidad de que el usuario final pueda interrumpir temporalmente la lectura del dispositivo?

R/. Con cualquier tecnología el usuario podría interrumpir temporalmente la lectura del dispositivo. La arquitectura propuesta utilizará cámaras de reconocimiento de placas para los vehículos que no cuenten con el dispositivo a bordo o si este no puede ser leído para asegurar un cubrimiento total de lectura.

P/. ¿Cuáles son las consecuencias si el dispositivo no puede ser leído por causa de una manipulación por parte del usuario.

R/. Referirse a la respuesta anterior, el sistema de cámaras entrará a actuar para identificar inequívocamente al vehículo.

MÚLTIPLES APLICACIONES.

P/. ¿El estándar ISO 18000-6c 2006 provee soporte técnico para múltiples aplicaciones?

R/. El estándar ISO 18000-6c define las capas 1 y 2 del modelo OSI, no define la capa 7 de aplicaciones. Como se explicó anteriormente, la arquitectura propuesta no utiliza la tecnología para la implementación de aplicaciones sino como identificación.

P/. ¿De qué manera se puede garantizar bajo la norma en cuestión la seguridad de la información, en lo que respecta a la confidencialidad e integridad en una arquitectura de sistema con múltiples aplicaciones (por ejemplo Identificación Electrónica Vehicular y Peaje Electrónico)?

R/. Como se explicó anteriormente, la arquitectura propuesta no utiliza la tecnología para la implementación de aplicaciones sino como identificación.

P/. ¿Quién es el responsable en un entorno de múltiples aplicaciones con autoridades e instituciones independientes en el caso que haya una violación a la seguridad de los datos del dispositivo?

R/. Como se explicó anteriormente, la arquitectura propuesta no utiliza la tecnología para la implementación de aplicaciones sino como identificación por lo que no almacenará ningún tipo de datos en el dispositivo.

P/. ¿De qué manera está organizada la arquitectura del sistema para accesar *(sic)* los datos de un dispositivo ISO 18000-6c 2006 en el caso de múltiples aplicaciones (por ejemplo Identificación Electrónica Vehicular y Peaje Electrónico)?

R/. Como se explicó anteriormente, la arquitectura propuesta no utiliza la tecnología para la implementación de aplicaciones sino como identificación, por lo que no es necesario organizar la arquitectura del dispositivo para acceder a los datos en ningún caso, incluyendo múltiples aplicaciones.

P/. ¿En caso que el dispositivo deba ser usado para Identificación Electrónica Vehicular y Peaje Electrónico, implicaría que diferentes autoridades o entidades deberían accesar *(sic)* el dispositivo para intercambiar información?

R/. Como se explicó anteriormente, la arquitectura propuesta no utiliza la tecnología para la implementación de aplicaciones sino como identificación. La interoperabilidad comercial se da mediante un conciliador nacional, no mediante intercambio de información almacenada en el dispositivo.