

Validação Conceito - Tags Digitais BLE

Validação do conceito de implementação de múltiplas arquiteturas sobre a mesma tecnologia e camada de transporte físico

Contexto

- O Sistema de Leitura de Transponders (SLT) utilizado nas pistas automáticas demonstra a capacidade de integração segura e padronizada com o mecanismo de Mensageria. Esse mecanismo (mensageria), bem estabelecido, pode de maneira eficiente, abranger a conexão com outros módulos de captura de dados e identificação veicular.
- O mecanismo de mensageria continua desempenhando um papel vital como elemento físico de ligação entre os dispositivos de captura de eventos de passagem de veículos e os sistemas de Gestão de Chaves e Mensageria.
- Tecnologias como Tags Virtuais (ou digitais) sendo executados em celulares podem ser alternativas para sistemas AVI, altamente escaláveis e econômicas

Contexto

- A inclusão de outras plataformas tecnológicas, como Bluetooth e WiFi, pode ser realizada sob as mesmas condições de utilização adotadas para tecnologias baseadas em câmeras e RFID.
- O requisito fundamental é que as implementações demonstrem segurança e eficiência na identificação, ou seja, leitura efetiva na passagem dos veículos pelo portal.
- As condições de passagem dos veículos em situações práticas devem ser consideradas nas certificações, incluindo:
 - Identificação eficiente em velocidades de até 160 km/h (ou outro valor considerado suficiente pela ARTESP).
 - Identificação eficiente de mais de um veículo do conjunto quando consideradas as condições normais de tráfego nos pontos de passagem nas rodovias.
 - Segurança na troca de informações garantindo comunicação segura (criptografada), mecanismos anti-clonagem e proteção de ataques como Replay Attack
- Este processo assegura que as diferentes plataformas tecnológicas atendam aos requisitos de identificação estabelecidos, garantindo eficácia e confiabilidade nas operações de monitoramento e gestão de tráfego

Contexto

- Esse relatório resume a validação de uma implementação de um Tag digital (aplicativo executado em celulares que utiliza Bluetooth como tecnologia de identificação RFID) realizada por uma empresa integradora*, diversa da já utilizada em algumas rodovias no país
- A implementação utiliza a mesma tecnologia de identificação do Tag Virtual já em uso do mercado (sem parar pay), ou seja, utiliza a camada física do padrão Bluetooth para transferência de dados
- Entretanto trata-se de uma implementação totalmente nova e distinta sendo realizada somente com base nas premissas descritos anteriormente
- Em resumo, mostra-se viável a homologação de novas implementações realizadas por empresas privadas, através de processos de homologação e validação sem que seja necessário análise (ou abertura) de detalhes do protocolo implementado ou do código fonte
 - Ressaltamos portanto, a recomendação de se permitir a liberdade de implementação por empresas privadas, não ser necessário padronizar os detalhes do protocolo de comunicação de cada implementação

* Empresa omitida por acordo de confidencialidade

Resumo conceitual

- A implementação validada apresentava as seguintes funcionalidades em seu protocolo de comunicação:
 - Identificador de chave: GID
 - Estrutura de mensagem com validação de integridade
 - Identificador do tag: OBUID (único e serializado de maneira segura através de EGC)
 - Dado variante no tempo: VARDATA e RANDA (dados gerados dinamicamente para garantir comunicação segura evitando ataques de Relay)

Resumo dos testes executados

- Foram executados a gravação e leitura de diversos Tags digitais
- Milhares de eventos de identificação foram gerados comprovando que as premissas de segurança e performance foram atingidas
- A nova aplicação não interfere em outras formas de identificação, podendo co-existir com outros Tags Digitais (ex. Sem parar-pay) e/ou outros sistemas de identificação (Como Tag RFID PA UHF)