Systemx
INSTITUT DE RECHERCHE TECHNOLOGIQUE

Accélérateur de la transformation numérique

Embedded Security Platform and Experimentations

Ines Ben Jemaa

seminar ISE @ETSI security week

16th of June 2017

ISE Experimentations Goals

- ✓ Vehicle's embedded security
- ✓ Penetration tests tools
- ✓ ISE PKI protocol

Implementation and validation of the ITS security mechanisms based on **ETSI standards**

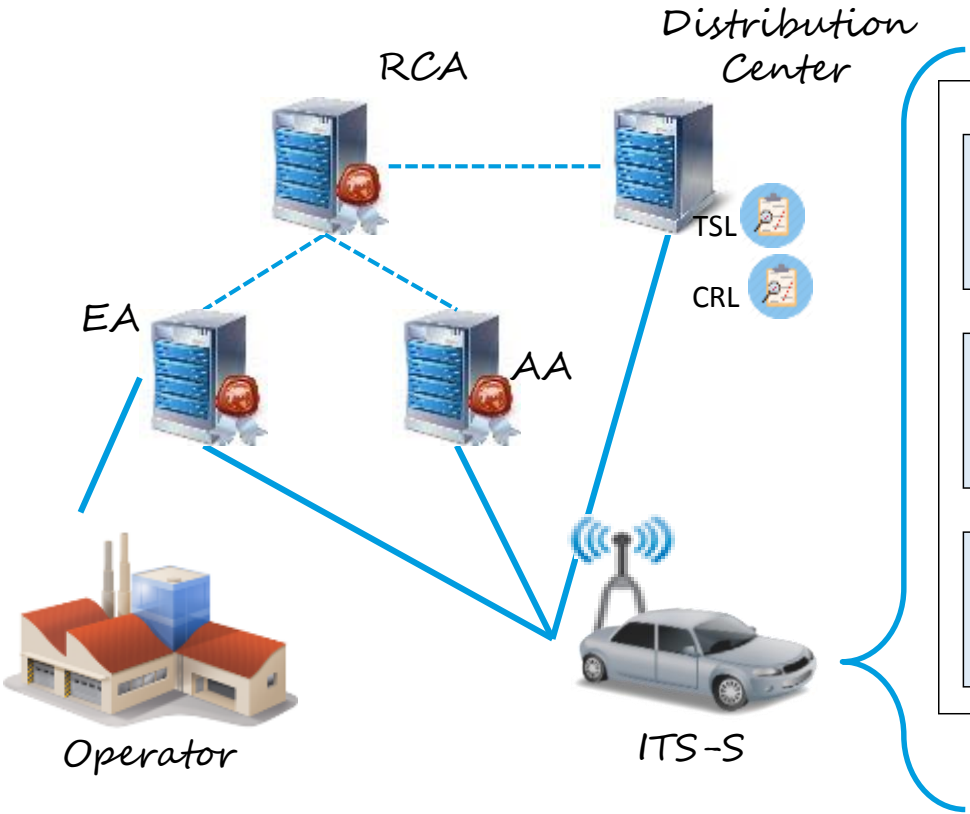
- ✓ Security stack performance
- ✓ PKI responsiveness

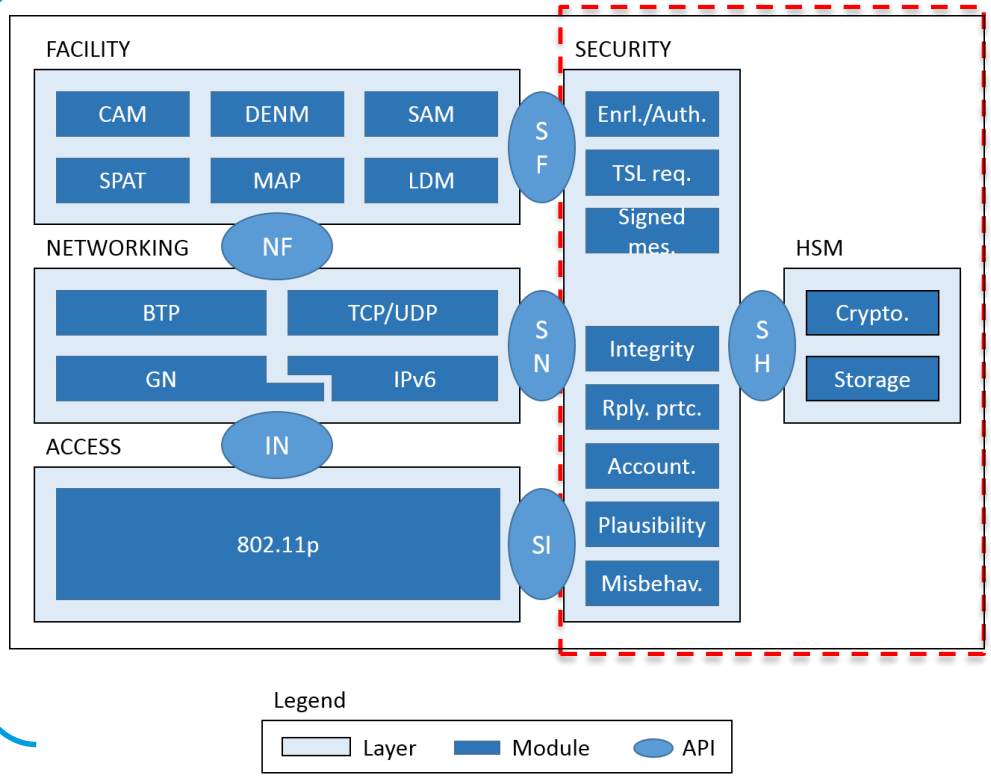
Performance evaluation of the security architecture

Contributions to the security standard development

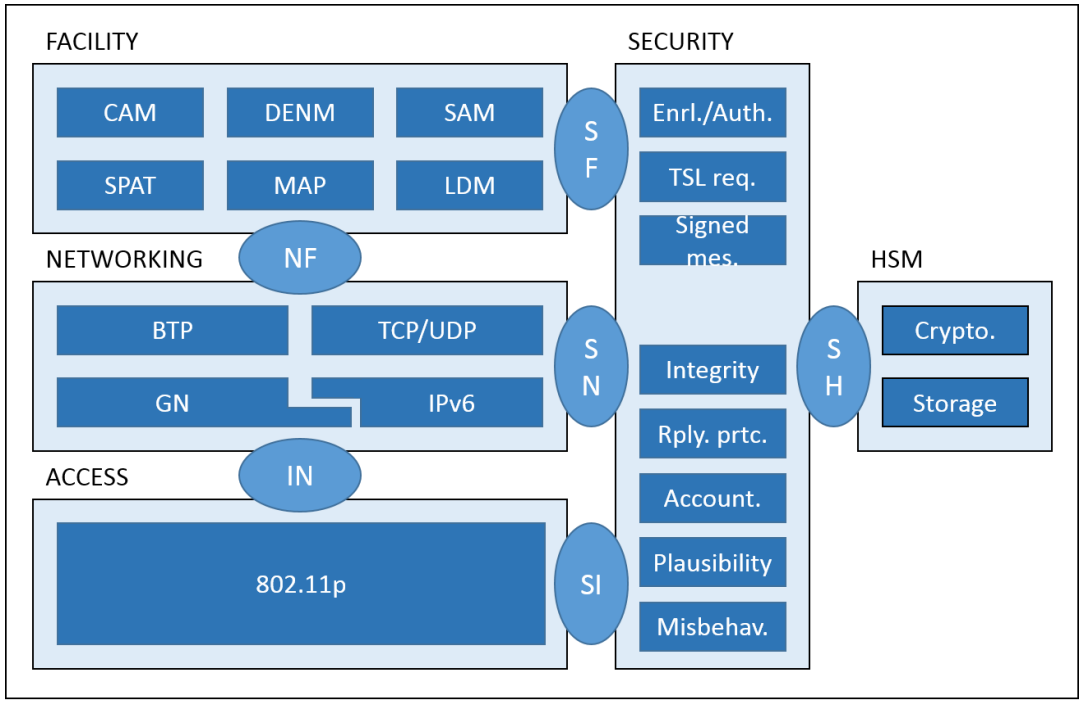
Effective transfer of research results to industry

On-Board Communication Architecture





Vehicular Security Modules



Implemented Modules

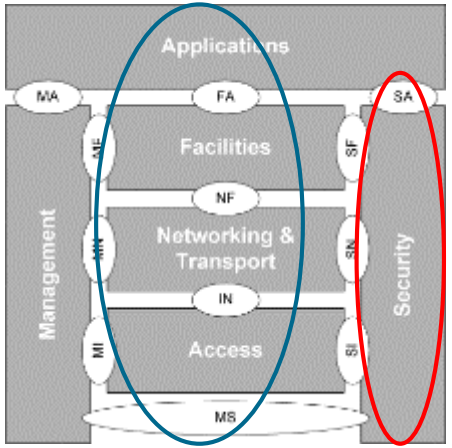
- Signature
- Verification
- Pseudonym change
- ITS-S identifier change
- Pseudonym reload
- TSL/CRL Request
- HSM integration

Implementation and integration

- **Hardware platform**
  - RENESAS OBU : 802.11p, HSM, GPS

- **Software platform**
  - YOGOKO Communication Stack
  - ISE Security modules
  - Applications : Authorization Ticket reloading, EEBL, SVW,

ITS-S architecture
(ETSI EN 302 665)



Vehicular Platform

On-Bord Unit

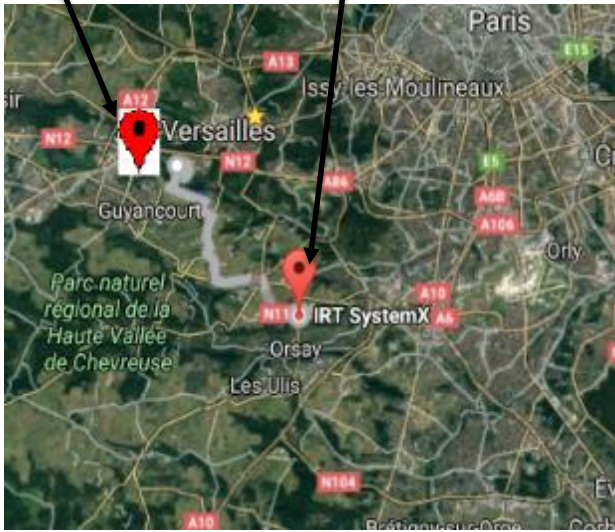
HMI

Raspberry PI 3

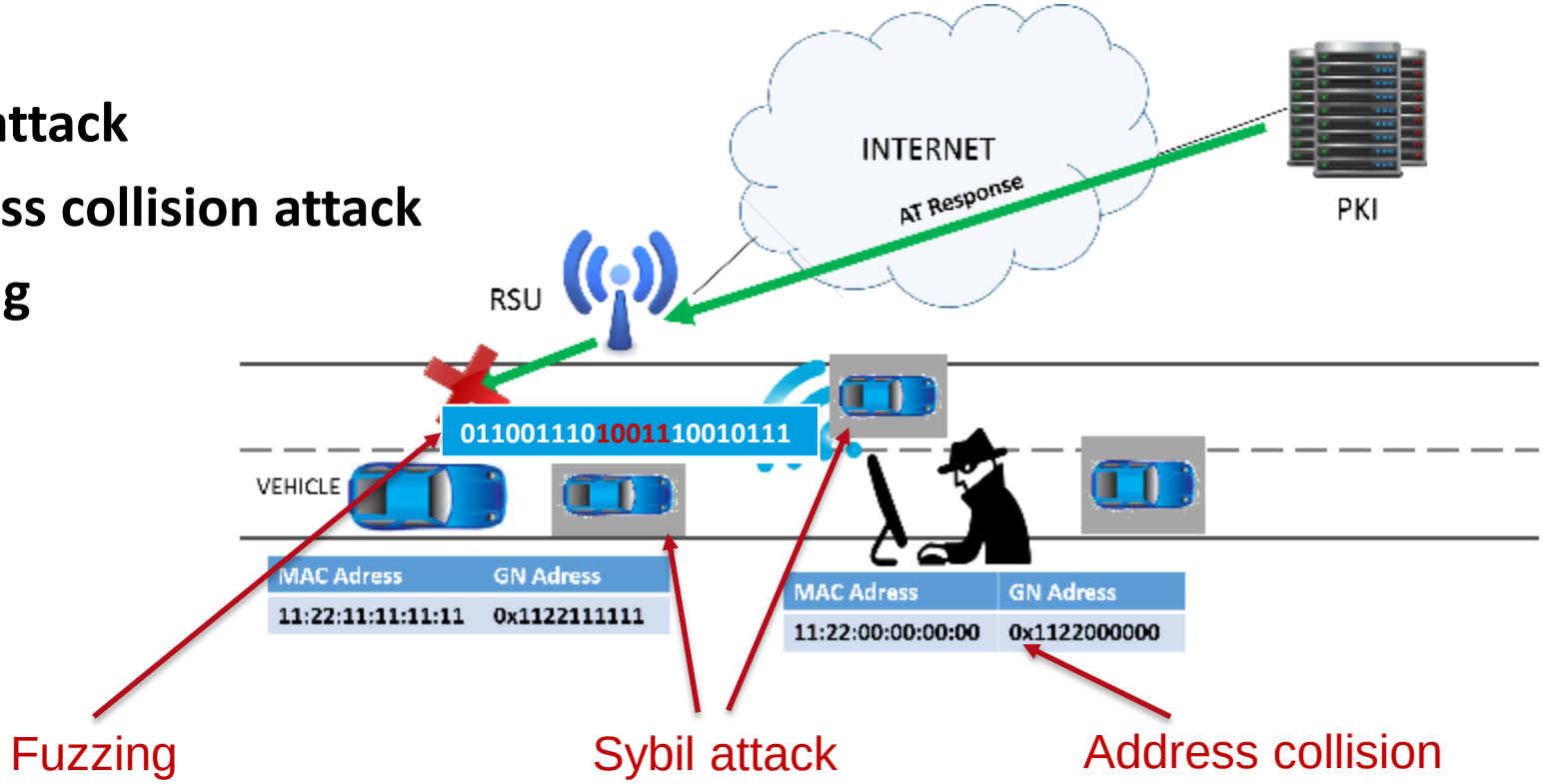
SystemX vehicle

Satory track tests

SystemX surrounding area

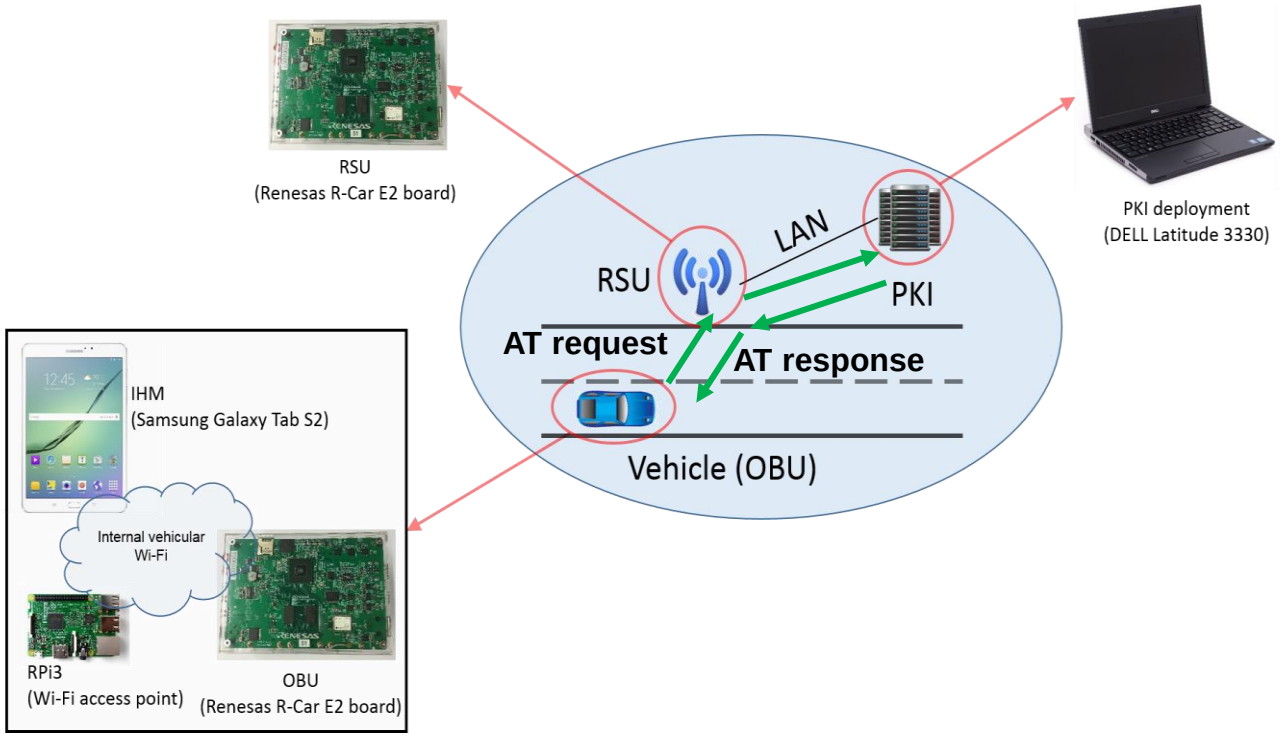


- Sybil attack
- Address collision attack
- Fuzzing



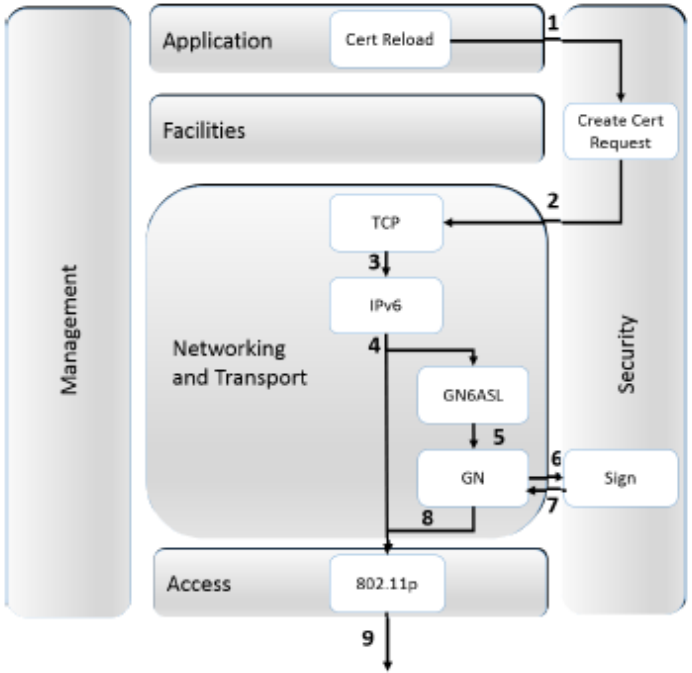
Authorization Ticket Reloading

- **PKI**
- **1 RoadSide Unit**
- **Vehicle**
  - OBU
  - Raspberry PI 3
  - Applications



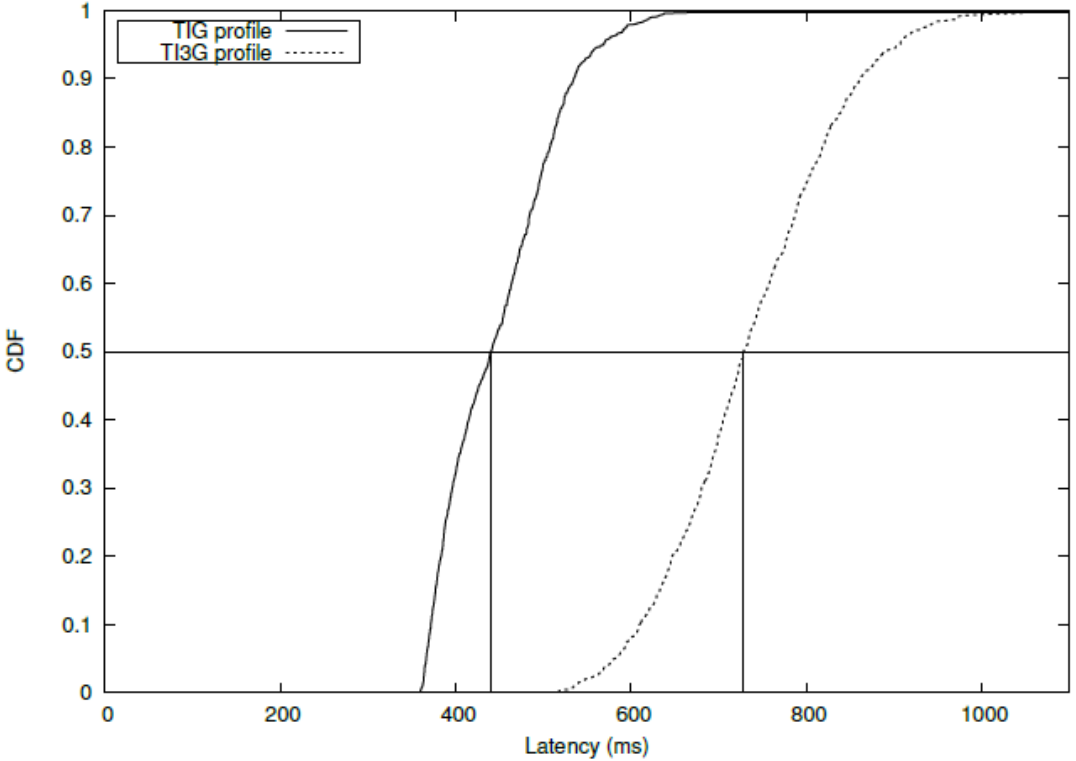
Performance Evaluation of the Authorisation Ticket Reloading Use Case

- **Communication profiles**
  - TCP/IPv6/G5 : “TIG” Profile
  - TCP/IPv6/GN6ASL/GN/G5 : “TI3G” profile
- **Extensive pseudonym reload experiments**
- **Performance evaluation**
  - Latency of the pseudonym reload operation



On the performance evaluation of vehicular PKI protocol for V2X communications security, Farah Haidar, Arnaud Kaiser and Brigitte Lonc, to be presented in VTC Fall September, 2017

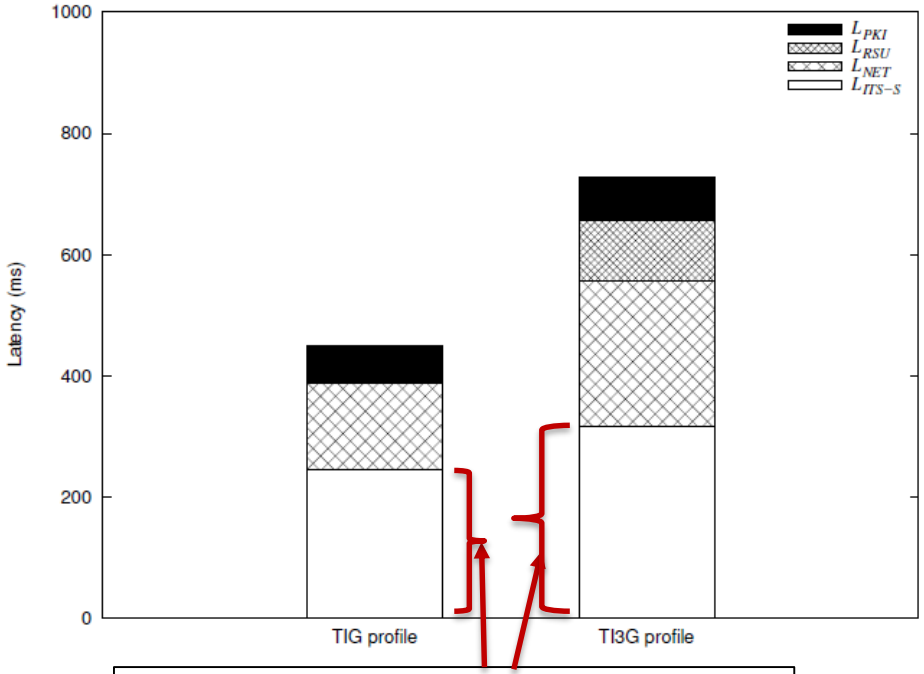
Latency Results (1/2)



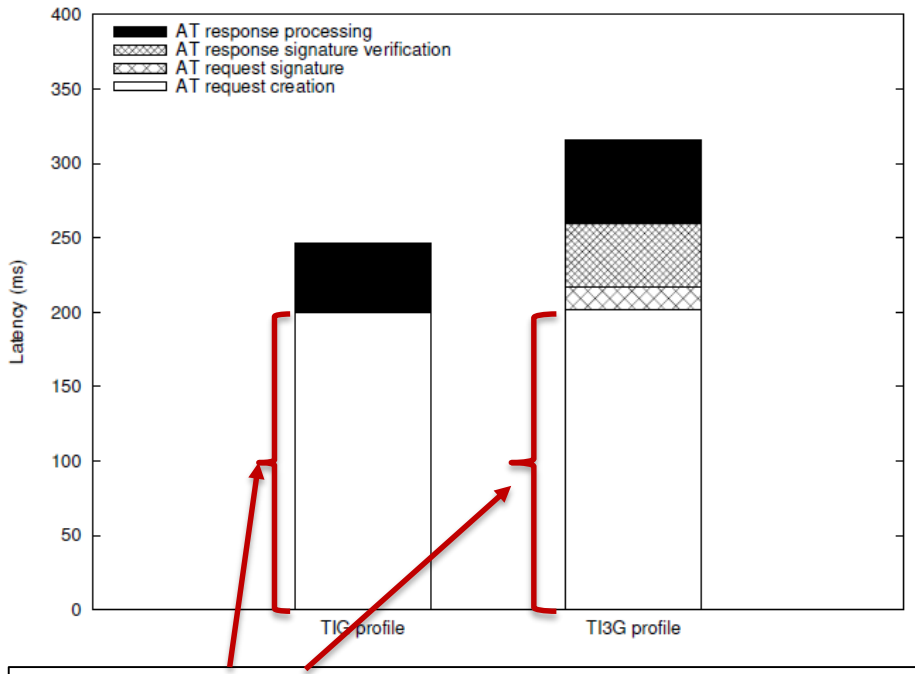
Average E2E Latency in TIG com. profile is around 0.45 sec

Average E2E Latency in TI3G com. profile messages is 0.7 sec

Latency Results (2/2)



The highest latency is at OBU processing operations

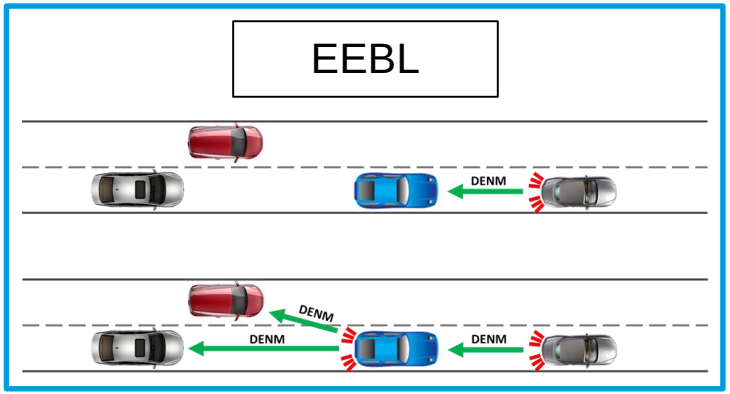


The AT request generates the highest latency

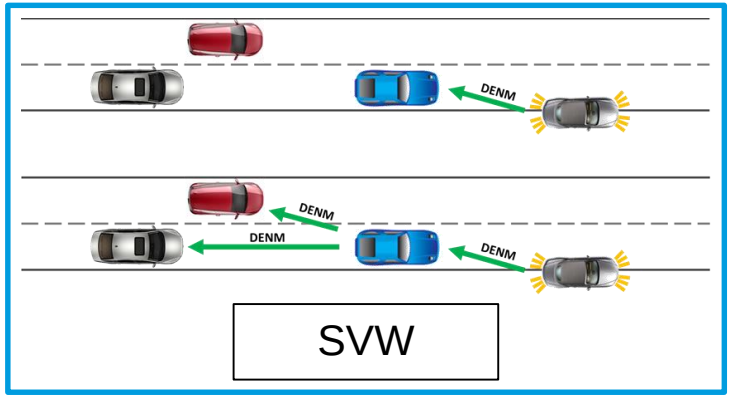
Tested Use Cases

Pseudonym Change lock

Emergency Electronic Brake Light EEBL



Stationary Vehicle Warning SVW



Summary

- **Proof of concept of the whole security architecture for C-ITS**
  - Embedded security
  - PKI protocol
  - ITS application
- **Indoor and outdoor experiments**
- **Current implementation requires some improvements**

Systemx INSTITUT DE RECHERCHE TECHNOLOGIQUE

Accélérateur de la transformation numérique

Thank you For your attention

Ines.ben-jemaa@irt-systemx.fr

www.irt-systemx.fr

Backup

Cooperative ITS Security Management System (CSMS)

- **PKI**
- **RoadSide Unit**
- **Vehicle**
  - OBU
  - Raspberry PI 3
  - IHM