Pillar 2: NEXTIUM, i2CAT, ATOS, Ubiwhere, UCY Multi-Radio V2X Communications Interoperability, Attack Detection and Mitigation

Jordi Casademont (i2CAT)

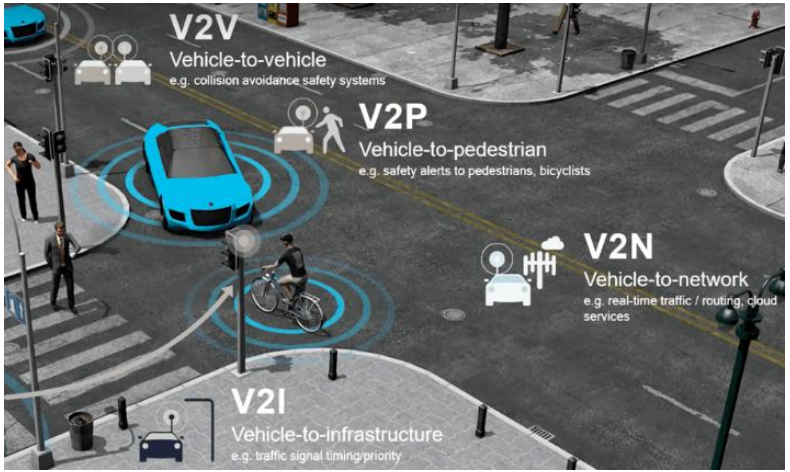
Barcelona, November 16th 2021

Agenda

- 1- Introduction to Connected Vehicle
- 2- CARAMEL Architecture
- 3- Use Cases
- 4- Conclusions

1- Connected Vehicle: Scenario

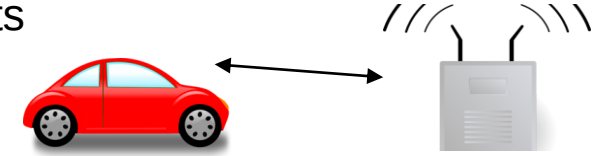
- Vehicle to Everything (V2X) communications



Source: Qualcomm

- Cooperative Intelligent Transport Systems (C-ITS)
  - Collision warning
  - Platooning
  - Lane-merging assistance

- System components
  - Hardware:

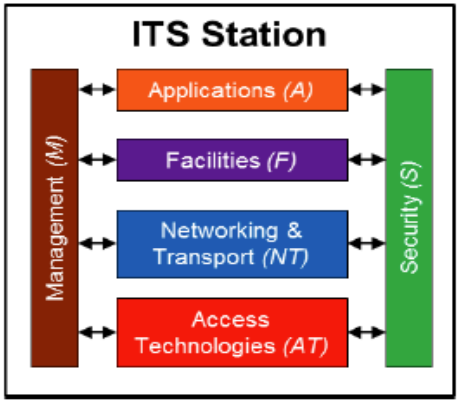


On-Board Unit (OBU) Road Side Unit (RSU)

  - Radio technology & Communication protocols
  - Security system: Public Key Infrastructure

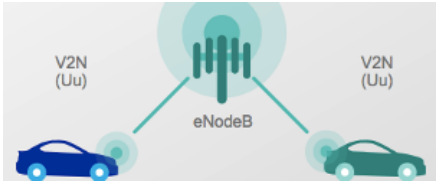
1- Connected Vehicle: V2X Communications

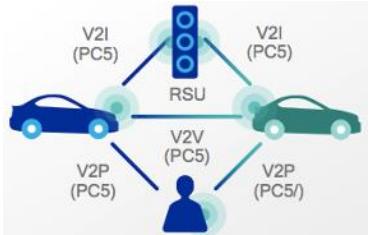
- New communication protocol architecture



- Networking and Transport
  - Europe: GeoNetworking
  - US: WAVE

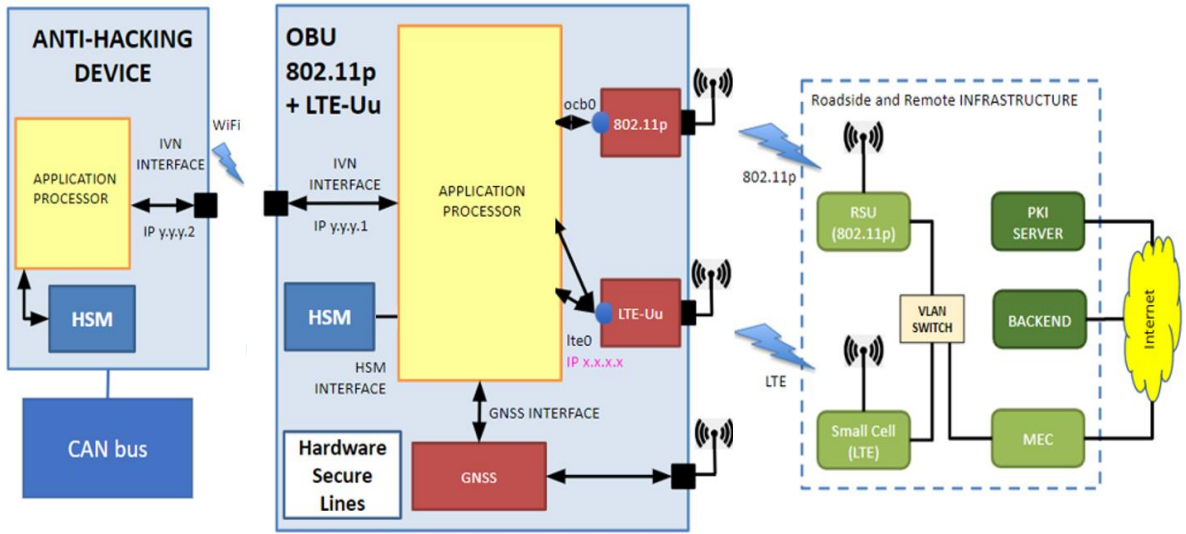
- Radio Technologies
  - Cellular channel (LTE-Uu) already available
    - Used to connect with PKI servers
  - IEEE: 802.11p (DSRC) - 2010
    - Very simple, based on CSMA/CA
  - 3GPP: LTE-V2X (C-V2X) - 2017
    - Larger coverage and slightly better capacity
  - All systems need to interoperate





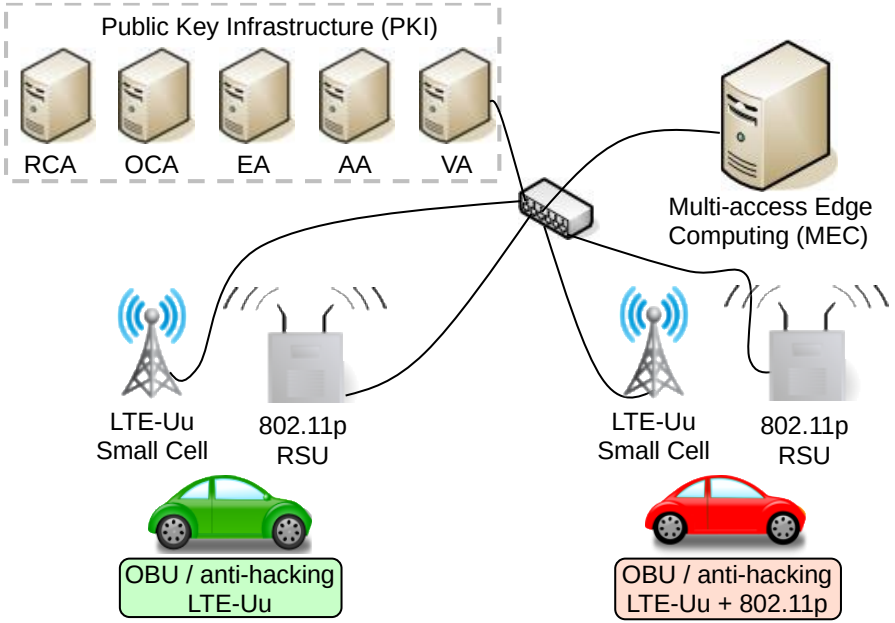
2- Architecture: Vehicle infrastructure

- Vehicle cooperative unit
  - On Board Unit (OBU)
    - V2X module (802.11p)
    - LTE module (LTE-Uu)
    - Security module (HSM)
  - Anti-hacking device
    - Additional security functions



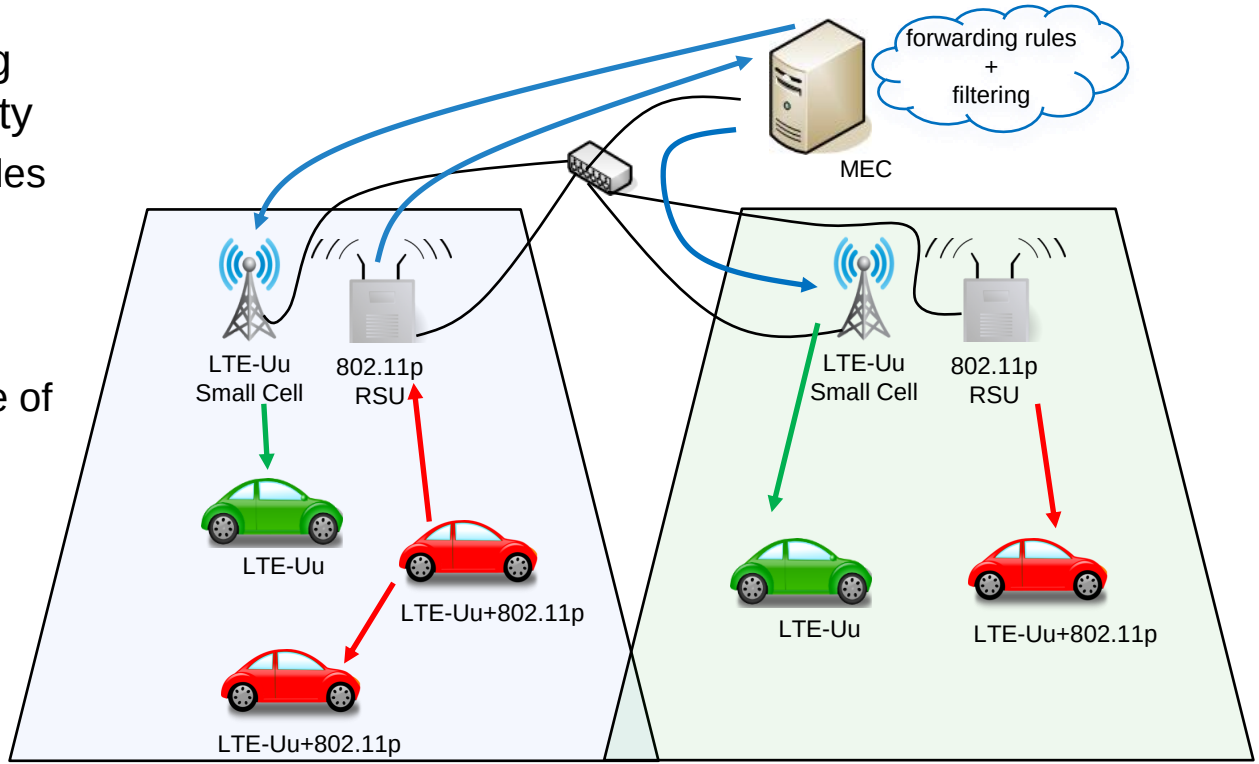
2- Architecture: Fixed Infrastructure

- Radiating road side units:
  - 802.11p RSU
  - LTE network (small cells)
- Public Key Infrastructure (PKI)
- Multi-access Edge Computing (MEC)
  - ETSI MEC framework standardization
    - Dashboard module / orchestrator / server
  - MEC functions:
    - Virtualization of V2X comm. stack
    - Radio technologies interoperability
    - Distribution of revoked certificates



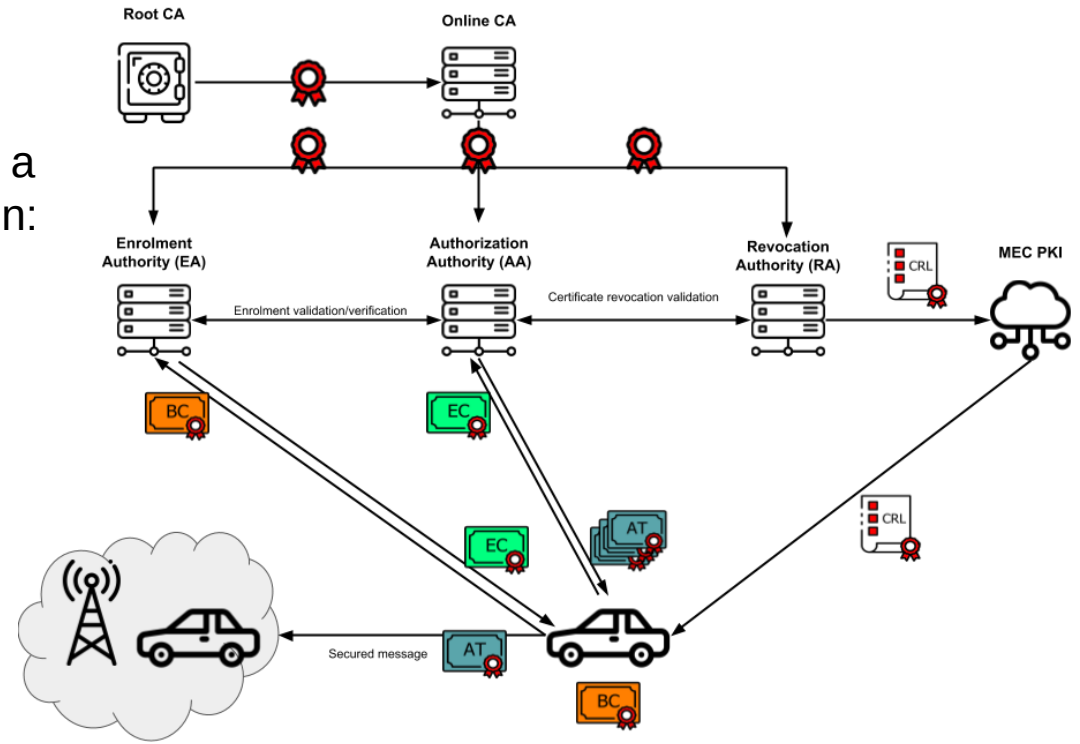
2- Architecture: Multi-Radio interoperability

- C-ITS Messages forwarding for multi-radio interoperability
  - Forwarding and filtering rules according to:
    - Region of interest
    - Age of the message
    - Validity of the signature of the message
    - Type of vehicle
    - Type of message



2- Architecture: Secure V2X communications - PKI

- PKI servers provide multiple certificates to the vehicles allowing a secured V2X message transmission:
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
  - Anonymity



3- Use Cases: Open problems for a secure C-ITS architecture

- Privacy reinforcement trying to avoid vehicle tracking
  - Compute the best instant to change AT and vehicle's addresses (MAC and GeoNetworking)
  - Machine learning techniques

- Attack detection
  - GPS spoofing attack: OBU broadcasts a false position
  - V2X message transmission attack
  - Tamper attack in the OBU: Hardware Security Module (HSM)

- Countermeasures:
  - If one car is under attack → Decide if it is prohibited from transmitting messages
  - PKI revokes certificates
  - Distribution of Certificate Revocation Lists (CRL)

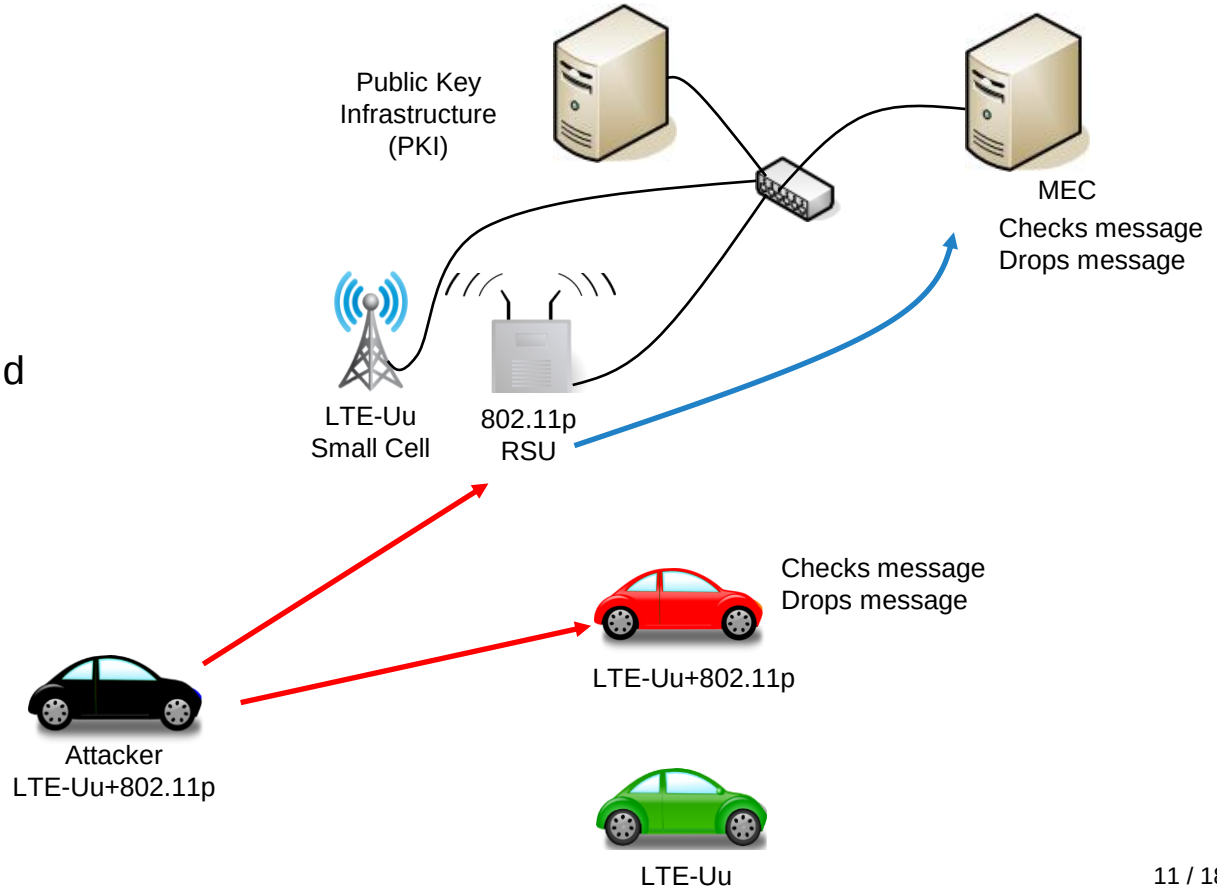
3- Use Case 1: GPS Spoofing attack

- GPS spoofing:
  - Receiver is attacked by injecting via broadcasting, incorrect GPS signals
  - Spoofed signals mislead the estimation process, predicting an erroneous position

- GPS spoofing attack detection:
  - Option 1: Executed locally in the vehicle: Self-localization integrity check
    - Uses other means to check the current position: cellular networks, accelerometers, steering angle, ...
  - Option 2: Executed externally in the MEC: collaborative position estimation
    - Vehicular network with vehicles in the road moving constantly and transmitting:
      - Absolute position, relative distance and angle of arrival measurements using LIDAR/RADAR
    - Multi modal optimization function can estimate the position of all the vehicles, taking those that have passed the integrity check as reference points

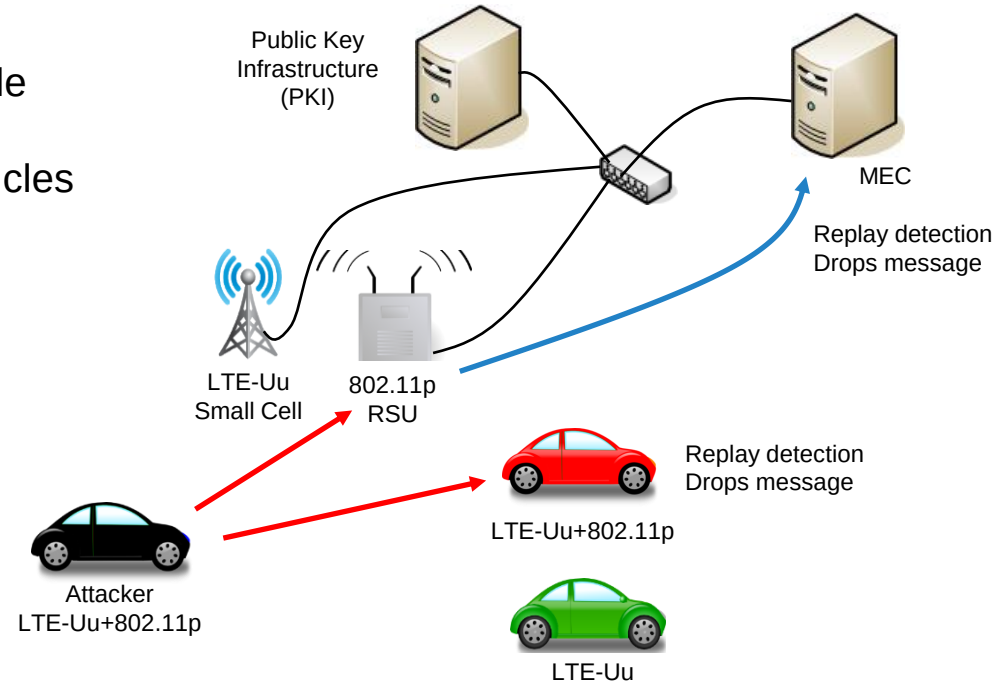
3- Use Case 2: V2X message transmission attack (I)

- Attack scenario 1
  - The attacker is a fake vehicle (without a valid certificate) that generates messages with some invalid data



3- Use Case 2: V2X message transmission attack (II)

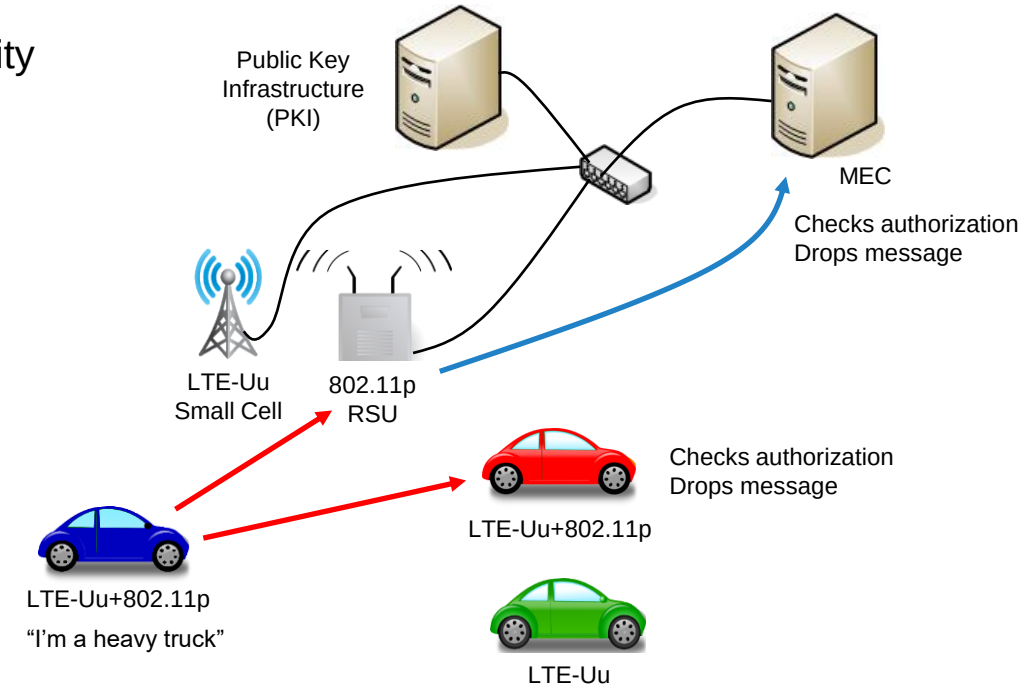
- Attack scenario 2
  - The attacker is a fake vehicle which sniffs and replays messages of compliant vehicles
  - Replay detection



3- Use Case 2: V2X message transmission attack (III)

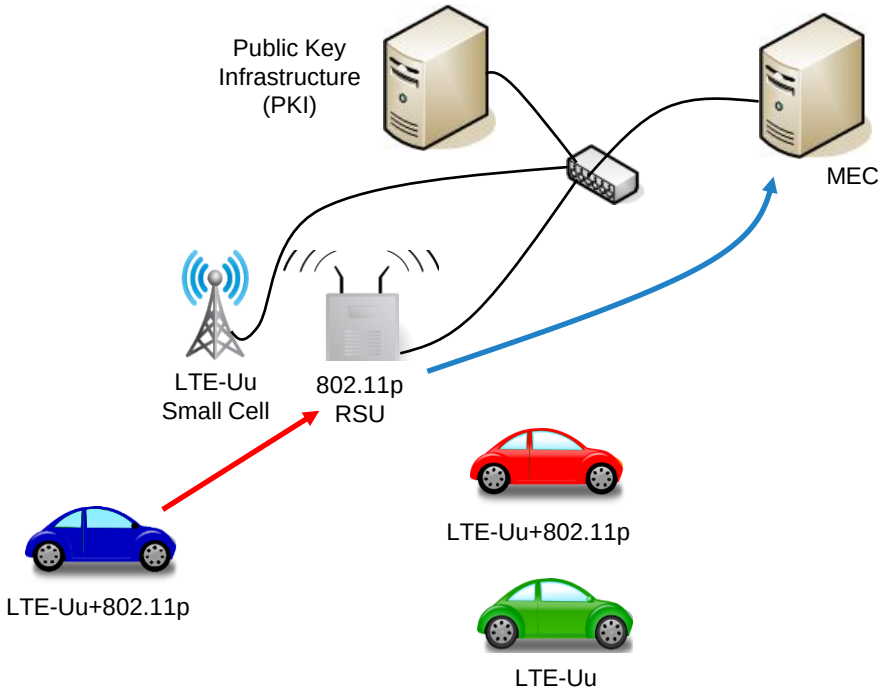
- Attack scenario 3
  - The attacker is a compliant vehicle but supplanting identity
  - Check Authorization versus type of ITS station

GeoNetworking Address
ETSI EN 302 636-4-1
ITS-S type.
To identify the ITS-S type.
0 - Unknown
1 - Pedestrian
2 - Cyclist
3 - Moped
4 - Motorcycle
5 - Passenger Car
6 - Bus
7 - Light Truck
8 - Heavy Truck
9 - Trailer
10 - Special Vehicle
11 - Tram
15 - Road Side Unit



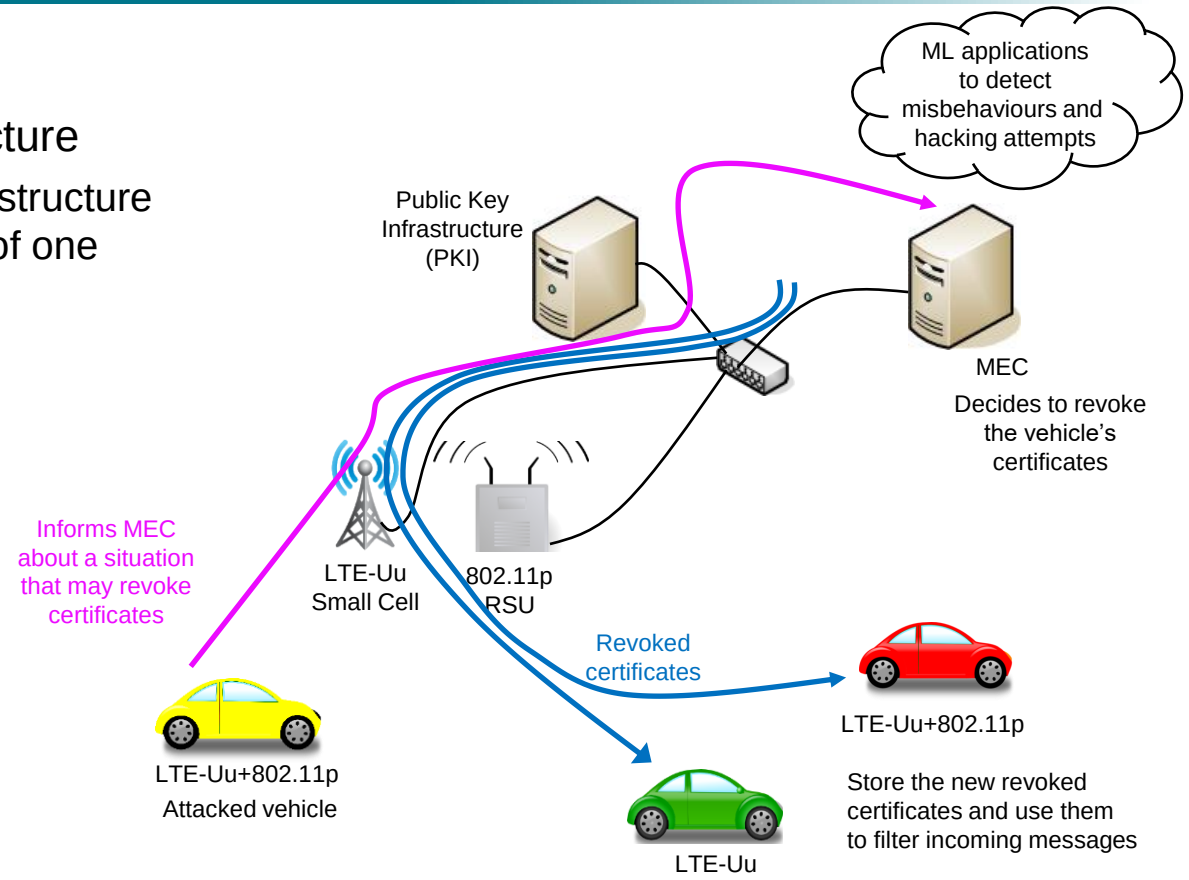
3- Use Case 3: OBU tamper attack

- OBU tamper attack:
  - OBU is manipulated in order to get access to secure information
- OBU countermeasures
  - Against environmental attacks (temperature, voltage and clock fault injection)
  - Against HW physical attacks
  - Against SW attacks



3- Use Cases: Certificate Revocation

- Detection in the infrastructure
  - One element of the infrastructure revokes the certificates of one vehicle
- Detection in the vehicle
  - Anti-hacking device
  - OBU's HSM
  - GPS spoofing
  - V2X message



4- Conclusions

- Collaborative Intelligent Transport Systems
  - Great perspectives of new services and applications based on vehicles positions
  - Currently developing new radio technologies that will require interoperability
  - Some services and applications are based on V2X communications, but others require fixed infrastructure network and computation capabilities

- Proposal of an architecture based on **MEC** and **Anti-Hacking Device** which provides:
  - Radio technology interoperability
  - ETSI compliant security: PKI infrastructure
  - Security improvements:
    - Tamper proof OBU with HSM
    - GPS spoofing attack detection
    - Certificate Revocation List distribution

CARAMEL

QUESTIONS ???

For further information, please contact:

Natàlia Porras Mateu
natalia.porras@nextium.com

THANK YOU FOR ATTENDING!!