chist-era

CHIST-ERA Projects Seminar
Topic SPTIoT: USEIT

Gregory Neven (IBM)

Nouha Oualha (CEA)

Antonio Skarmeta (UMU)

Paris, April 11-12, 2018

FUNDING OPPORTUNITIES from the FUTURE & EMERGING TECHNOLOGIES scheme

USE-IT

- **USE-IT:**

  User empowerment for **SE**curity and privacy
  in **I**nternet of **T**hings
  http://useit.eu.org

- **Aim:**

  To let users and devices easily and tightly control who has access to which data in which context, without leaking collateral information such as location or behaviour data.

- **Duration:**

  36 months (Feb 2017 – Jan 2020)

USE-IT Partners

- **IBM Research – Zurich, CH:**

  coordinator, focus on cryptographic protocol design for constrained devices

- **University of Murcia, ES:**

  focus on advanced access control solutions and privacy-preserving authentication for IoT

- **Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA), FR:**

  focus on reactive security technologies enabling attack detection and reconfigurability of communication security

- **Technical University Eindhoven (TUE), NL:**

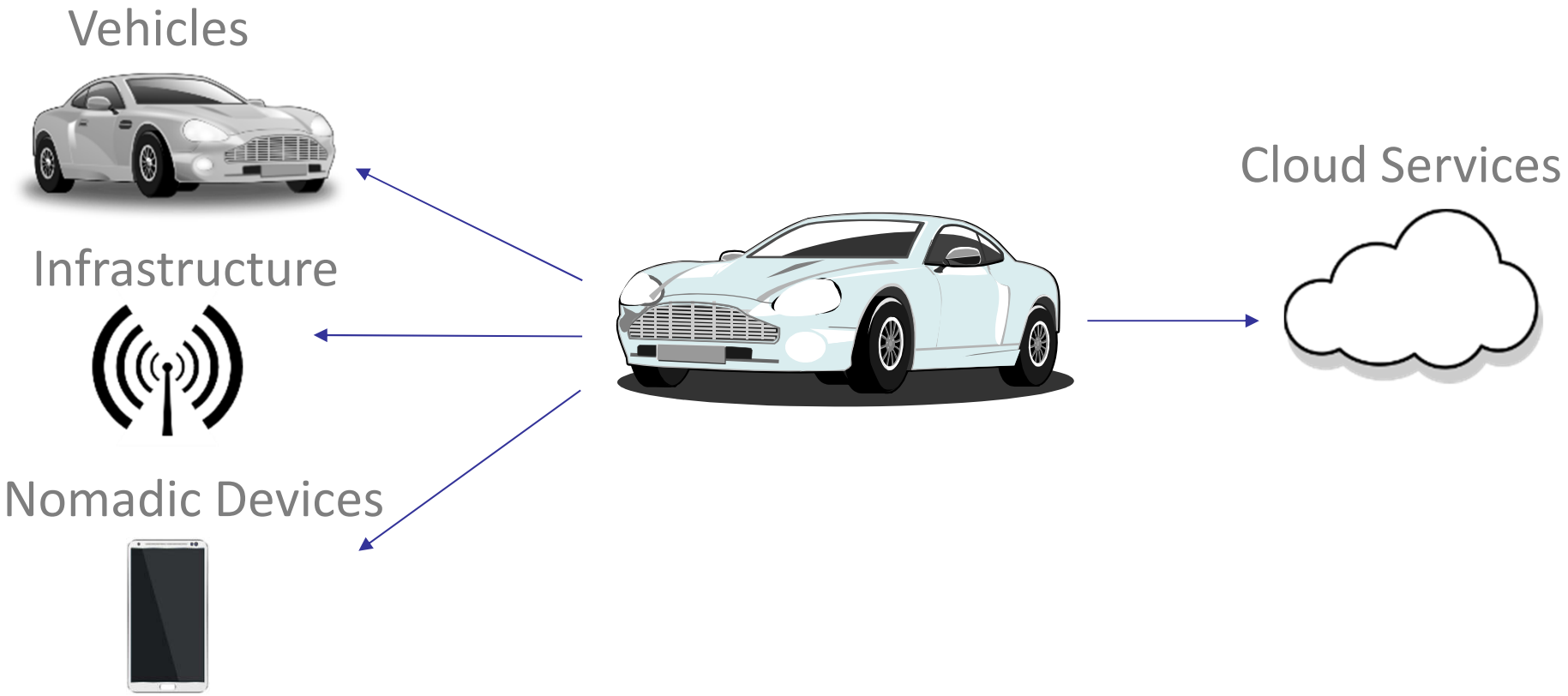
  focus on design and evaluation of cryptographic protocols and in efficient implementations

USE-IT Objectives

- Design **new privacy-preserving authentication and encryption schemes** for constrained IoT environments
- Create **simple policy languages** to govern crypto protocols and access control
- Implement new tools for **informed consent** that work within limitations of IoT
- Develop powerful, flexible, lightweight **intrusion detection/ reaction for IoT**
- Integrate the developed technology into existing frameworks and applications to **viability in the real world**
- Use **rapid prototyping** to implement

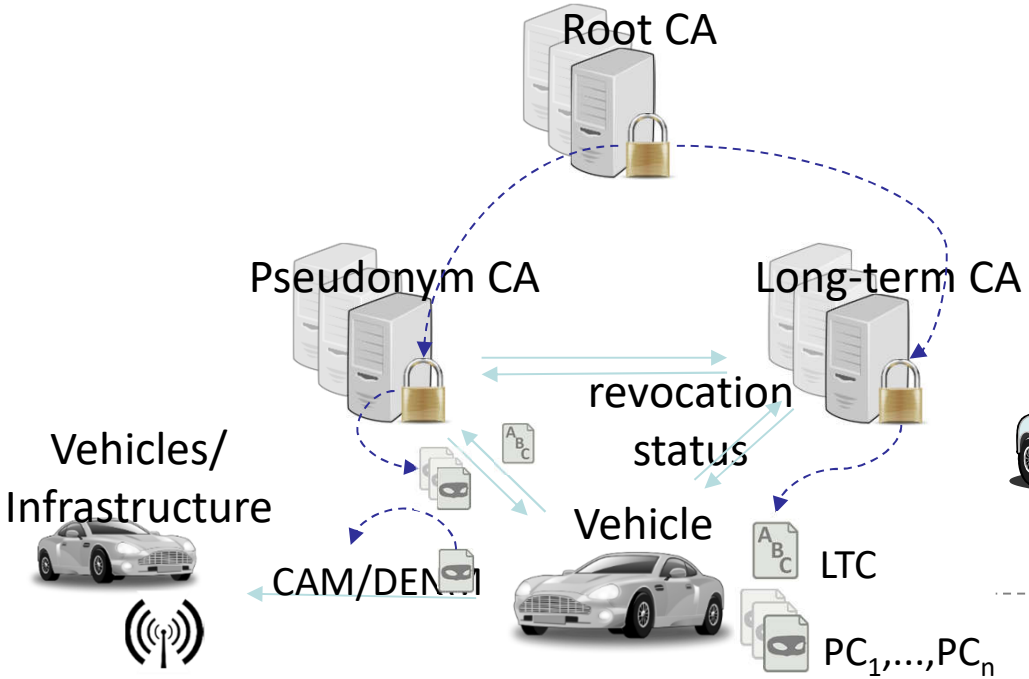
Use Case 1: C-ITS

- **Cooperative Intelligent Transport Systems (C-ITS)**
  - ✓ CAM: location beacon messages
  - ✓ DENM: environment/hazard notifications

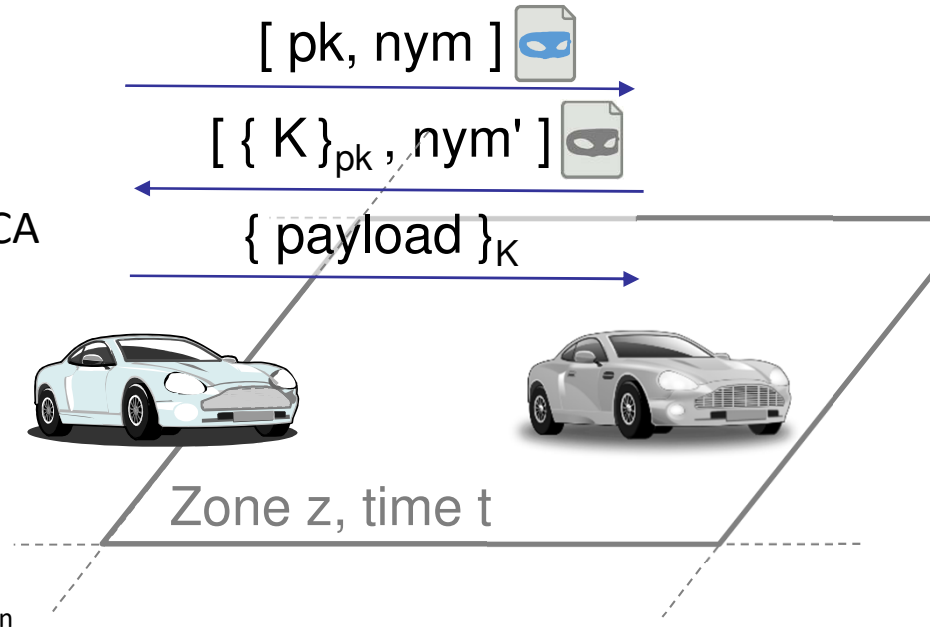


C-ITS Solution

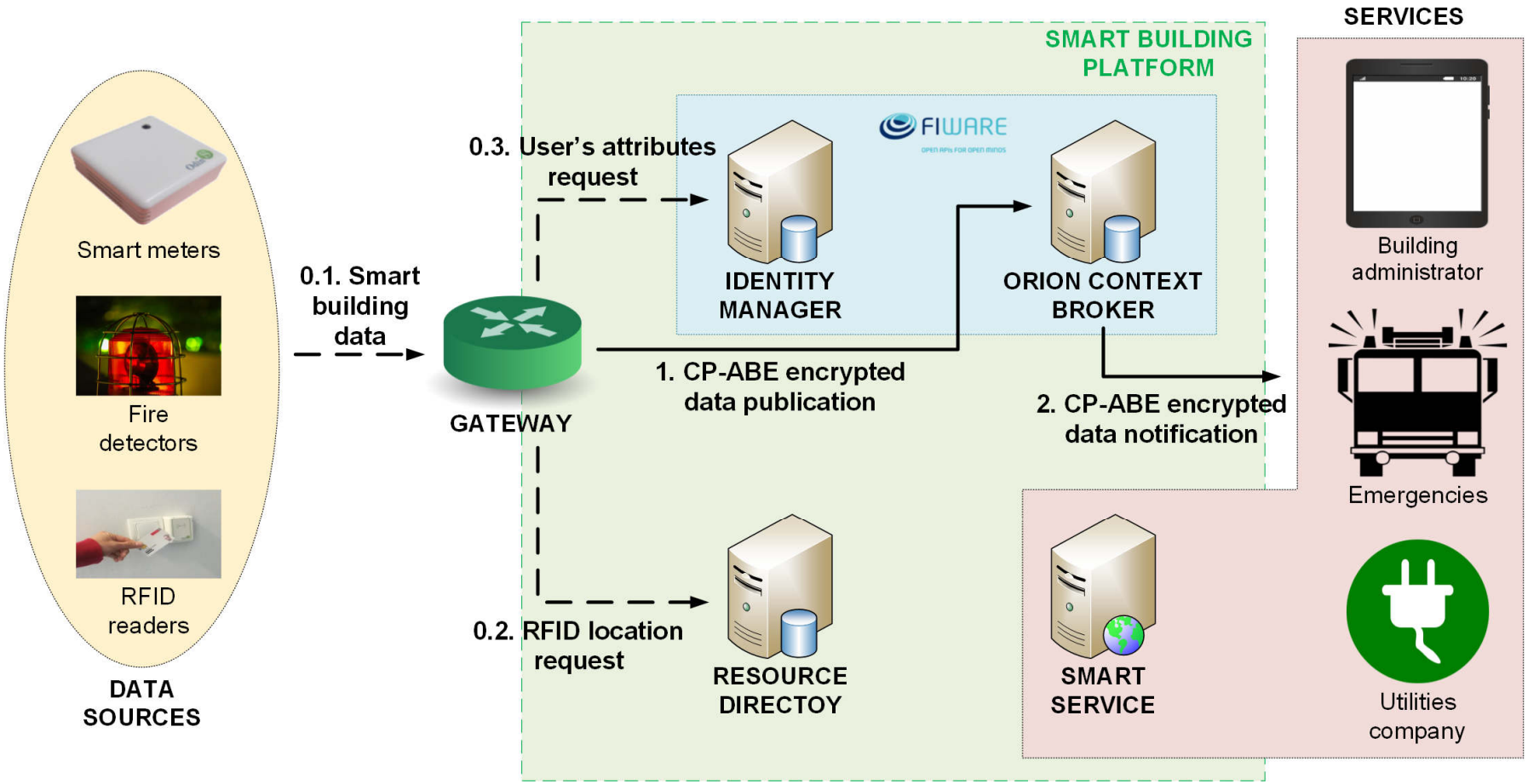
Privacy-ABCs for unlimited pseudonyms



Geo-zone encryption for location privacy



Use Case 2: Smart Building



Smart Building Solution

- To combine symmetric key cryptography to protect data, with CP-ABE to distribute the symmetric keys, thus achieving a trade-off among scalability, efficiency and flexibility
- Techniques based on pre-computation and re-encryption to reduce computation end energy costs of ABE encryptions
- Accommodate CP-ABE to IoT scenarios with resource-constrained devices sharing huge volumes of data
- Building new and profitable bridges between incident response (reactive security) and attribute-based (preventive cryptographic) security by integrating intrusion detection and reaction system to the use case

The Road Ahead

- **Finish cryptographic design**
  - ✓ protocols
  - ✓ pairing curves to use
- **Integration**
  - ✓ geo-networking protocol with C-ITS security protocol
  - ✓ smart buildings: intrusion detection and CP-ABE
- **Testbed implementation & validation**