Automotive-PKI for C-ITS

autotech. agil

With funding from the:
Federal Ministry of Research, Technology and Space

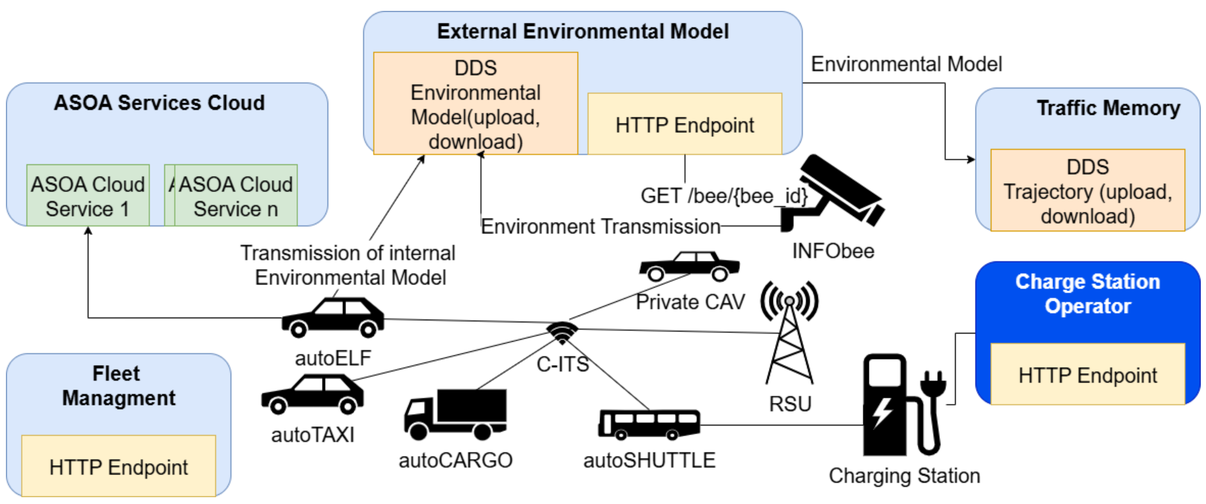
Trust anchor for C-ITS communication

Critical resources and attack targets require cryptographic security

- TARA in line with UN/ECE 155 and ISO/SAE 21434
- Attack targets:
  - Personal data, influencing traffic flow, jeopardizing the safety of a vehicle
- Resources to be protected:
  - Vehicle integrity, traffic infrastructure, positions, vehicle signals

Defense Strategy in the C-ITS Ecosystem

- Protection of intra-vehicle and external-communication.
- PKI integration for automotive ecosystems.
  - Providing Trust anchor for:
    - ASOA, V2X and Charging
- A security gateway enabling secure V2X (Universität Passau).

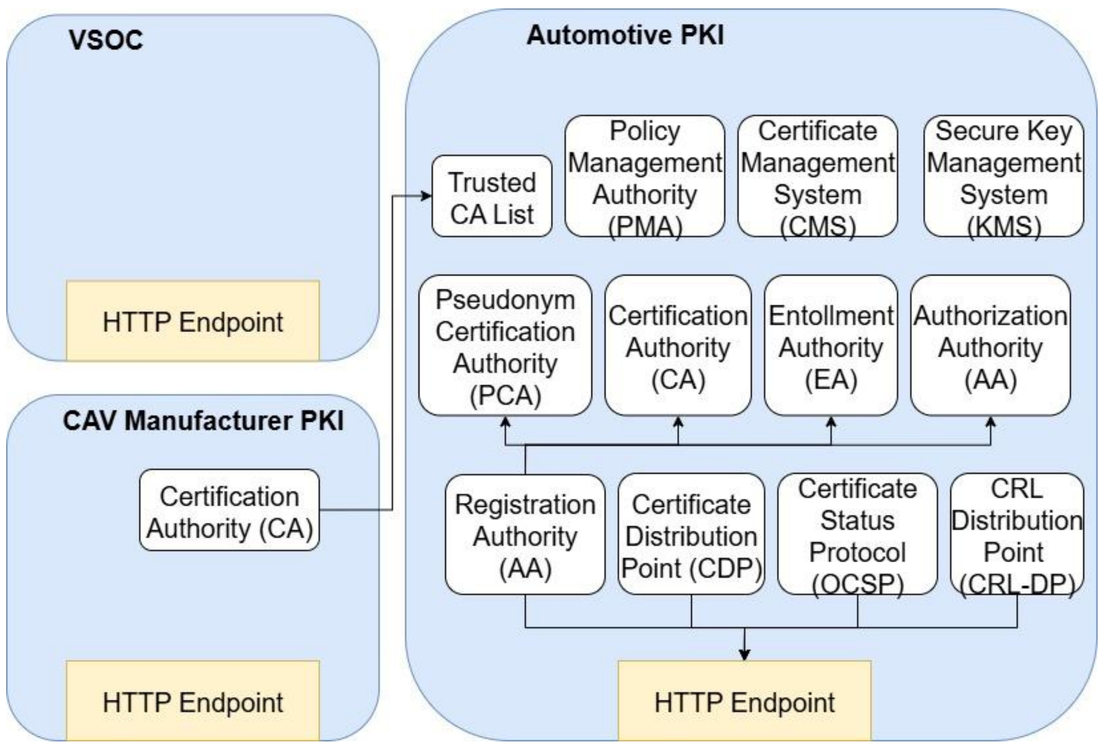


Integration into the C-ITS Ecosystem

- Harmonization of PKIs for
  - C-ITS
  - EV-Charging
  - Cloud communication
- Surrounding environmental data
- Live PKI for certificate renewal of vehicles, RSUs, and backends
- Role and authorization model of multiple PKI instances

Certificates in the ETSI model

- Enrolment certificates (identity)
- Authorization certificates (roles & rights assignment)



Life Cycle Management of Certificates

- Secure Creation of Certificates
- Usage and Distribution of Certificates
- Revocation of Malicious Certificates
- Generate Pseudonymized Certificates

Challenge & open questions

- Introduction of PQC:
  - NIST standard not compatible with C-ITS
  - Few signature candidates Relevant:
    - MAYO, SNOVA, UOV
  - Interoperability (EU-wide use)
  - Privacy vs. security

Contributing Partners

INCYDE

UNIVERSITÄT PASSAU