Data Truthfulness and Software Integrity for ITS

PODIUM Webinar

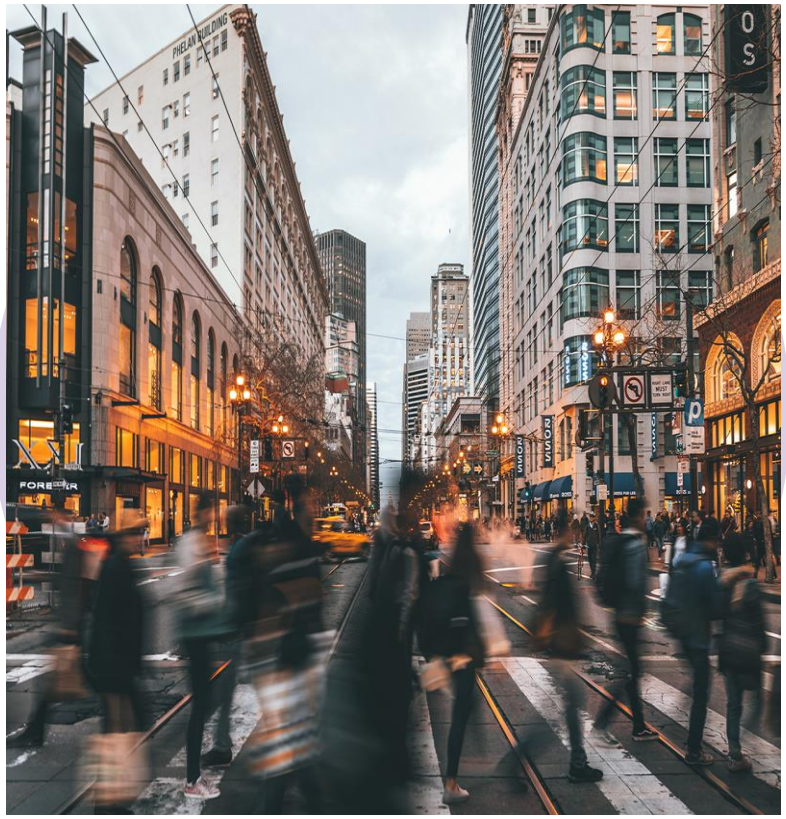
November 30th 2023

Guido Gavilanes
LINKS Foundation

Brussels, 22 January 2023

Co-funded by
the European Union

Trust vs Truthfulness



Both answer this question:

How can CAVs and algorithms rely on what the PDI says?

- Sensor data might be false positives
- Road user's data idem, and any user with radio access can send ANY data
- Elaborated results from these data

We can split this question in two:

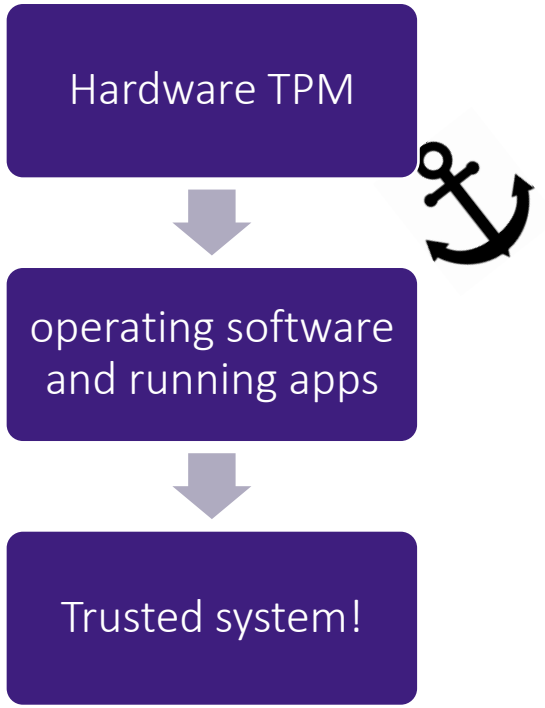
1. Are the data users/sensors really who they claim to be?
2. Is what PDI receives from users/sensors true?

Trust 1

Truthfulness 2

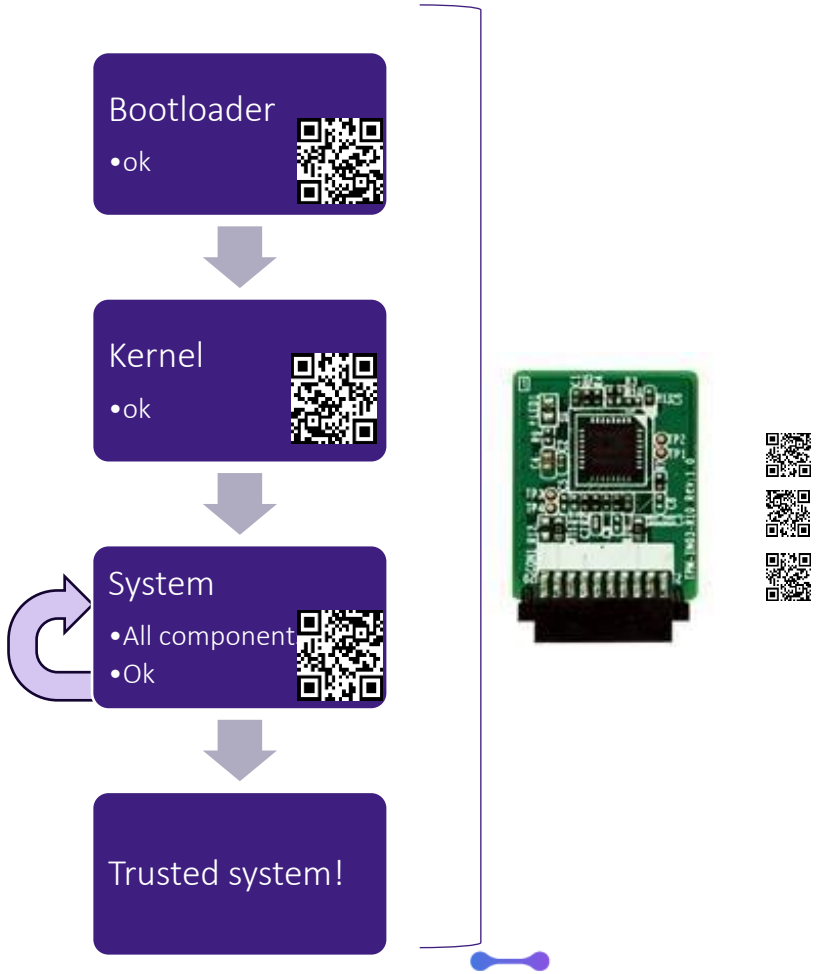
Trusted Computing strategy

- Trusted Computing (TC) is a set of interoperable technologies to achieve a level of trust in the behaviour of a device.
- The core element of TC is the hardware **Root of Trust** called Trusted Platform Module (TPM) a tamper-resistant cryptographic hardware integrated with the system board, able to perform cryptographic primitives. (TCG specification TPM 2.0).
- The objective of TC is to enable devices to measure and prove their integrity cryptographically, *i.e.*, prove that their running software is the intended one and it has not been tampered with, to the other devices involved in the network.

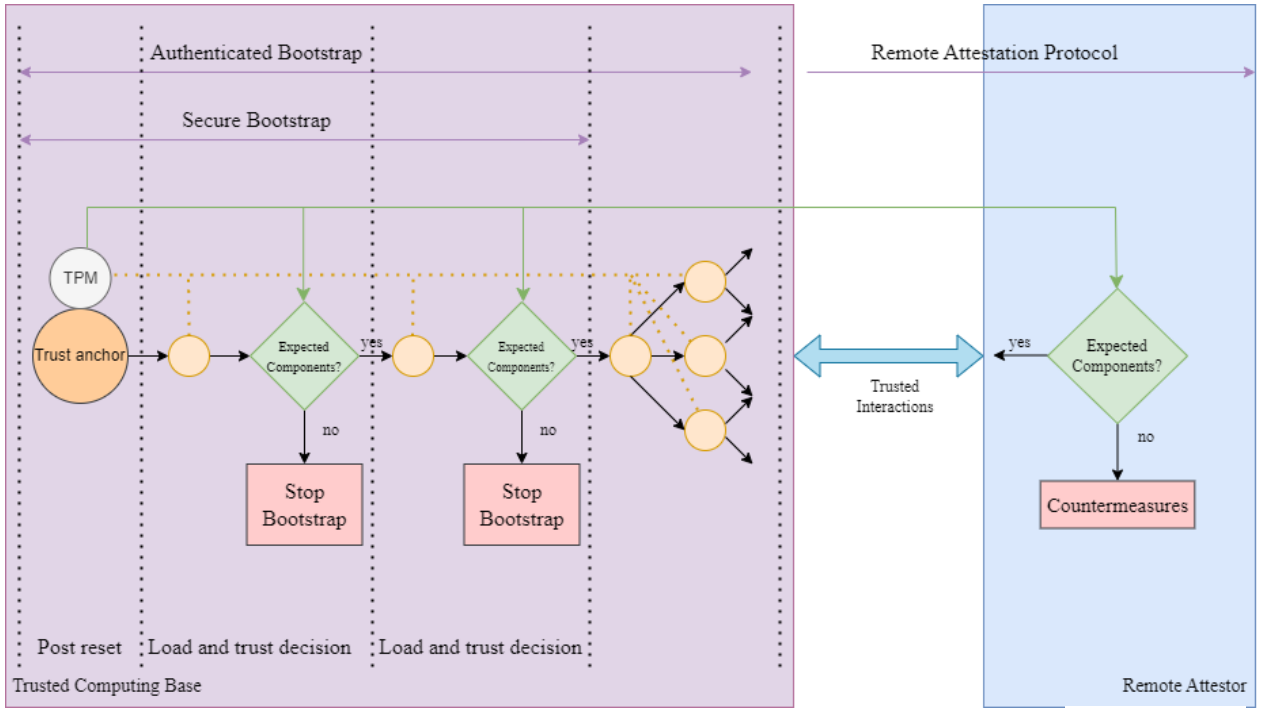


Software integrity architecture (I)

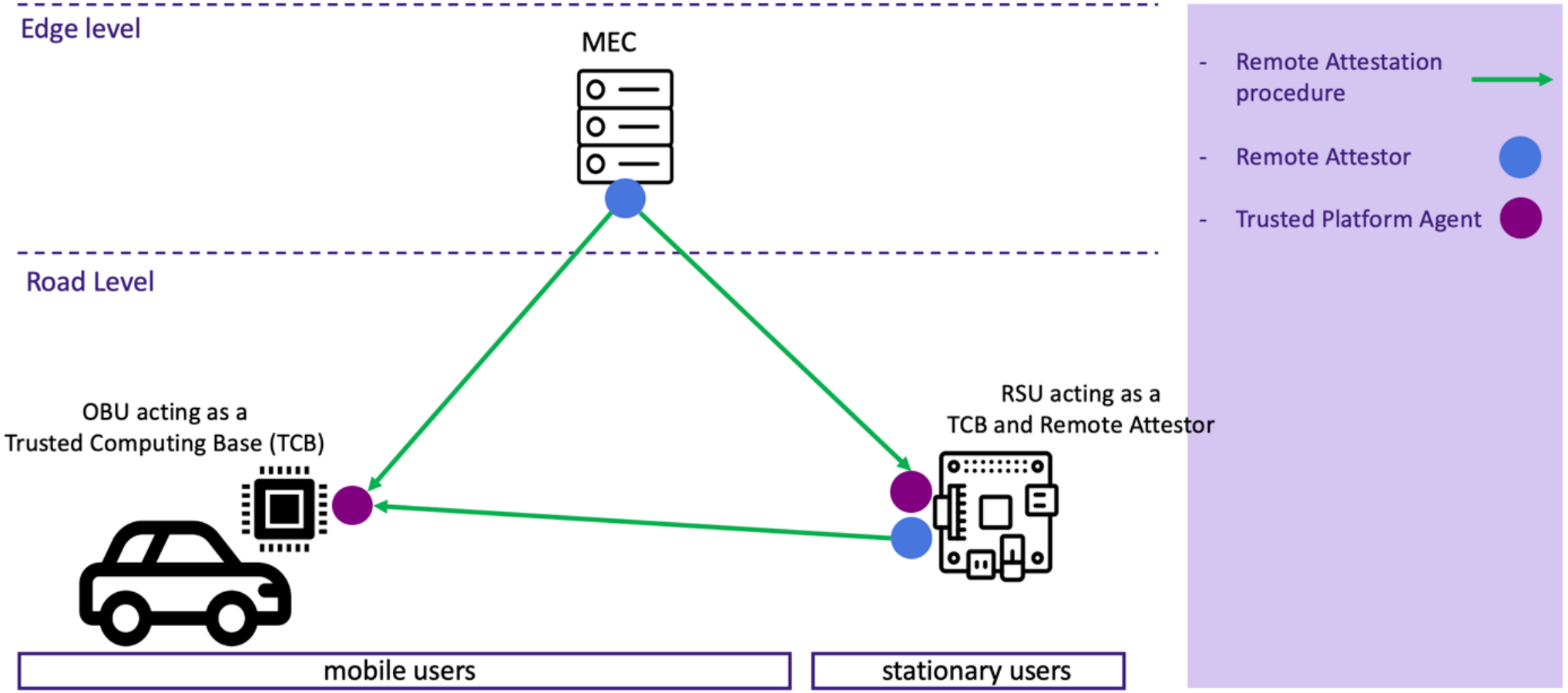
- The software architecture is responsible for building the Chain of Trust and enabling 3 trust decisions:
  - two at boot time (on the integrity of bootloader and then on Linux kernel)
  - one at runtime (on the integrity of applications/services) through periodic remote attestation.



Trusted Computing OBU

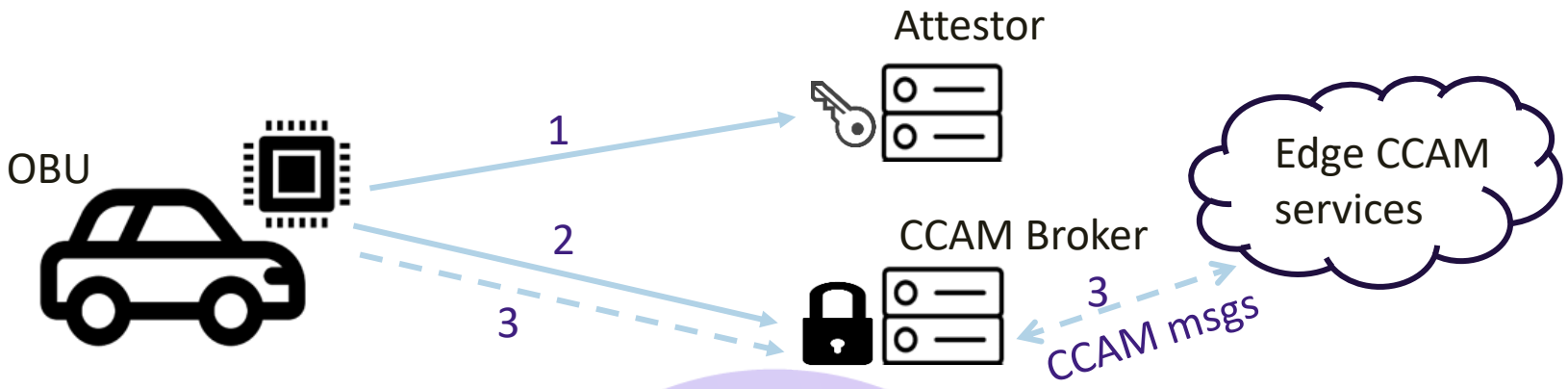


Trusted Computing in PODIUM



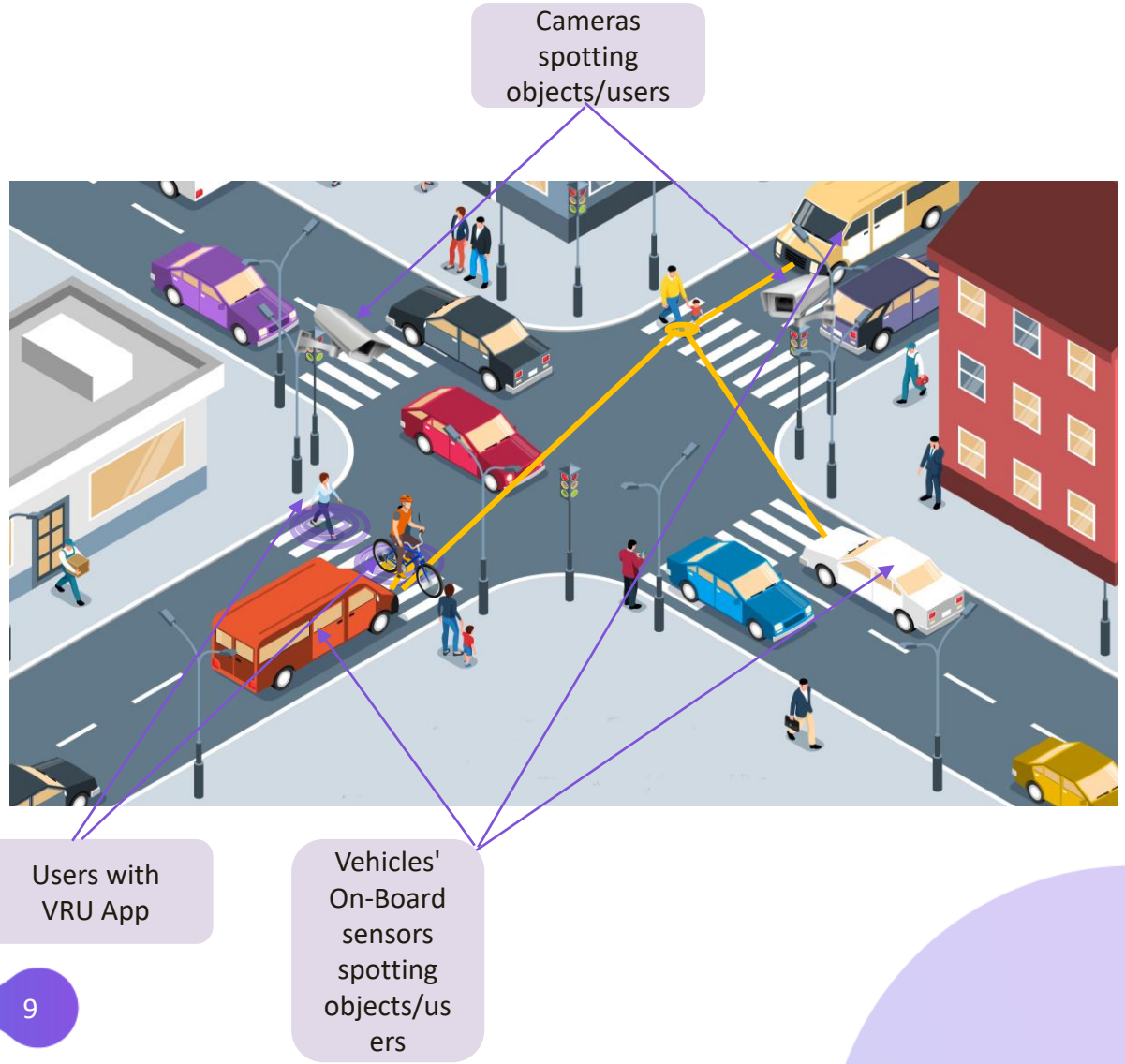
From untrusted to trusted OBU

- OBUs transmit **CCAM** messages to interact with edge/cloud services
- In the service discovery phase, an attestor is in the middle to provide proper credentials to use CCAM broker
- Credentials are **valid** while attestation is **positive**



Truthfulness

Truthfulness 2



- Is information reliable? There are two substrategies:
  - **Self-assessment of fusion module.**
    - Checks data/statistical assumptions with subjective logic
  - **Redundancy based sensor data fusion**
    - Ranks information in truthfulness levels according to the redundant sources that originated the same information.

Data Truthfulness Strategy

Is that a pedestrian?

Is that a vehicle?

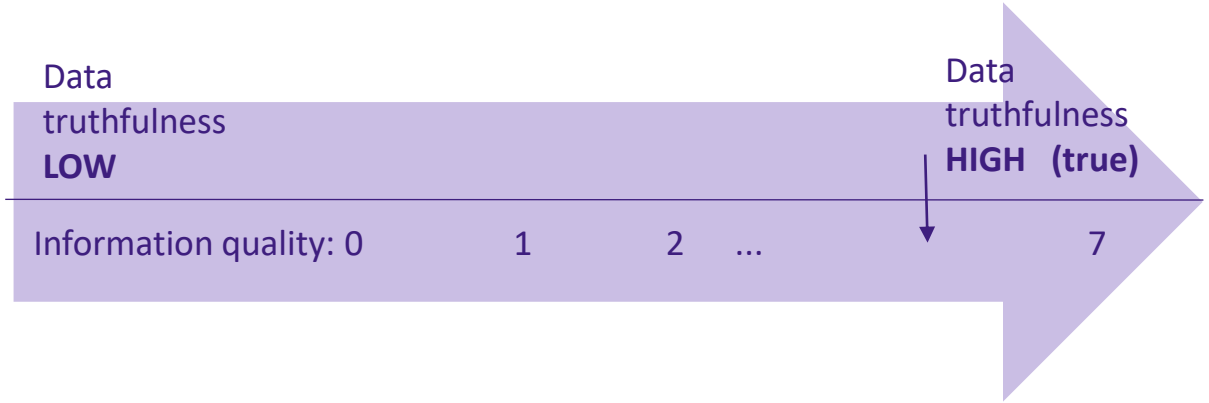
CPM message arrives from CAV Containing a bicyclistAndLightVruVehicle on the pedestrian lane

A VAM message arrives, announcing VRU position

Camera detects a pedestrian and cyclist on the lane

Higher probability that a cyclist is present

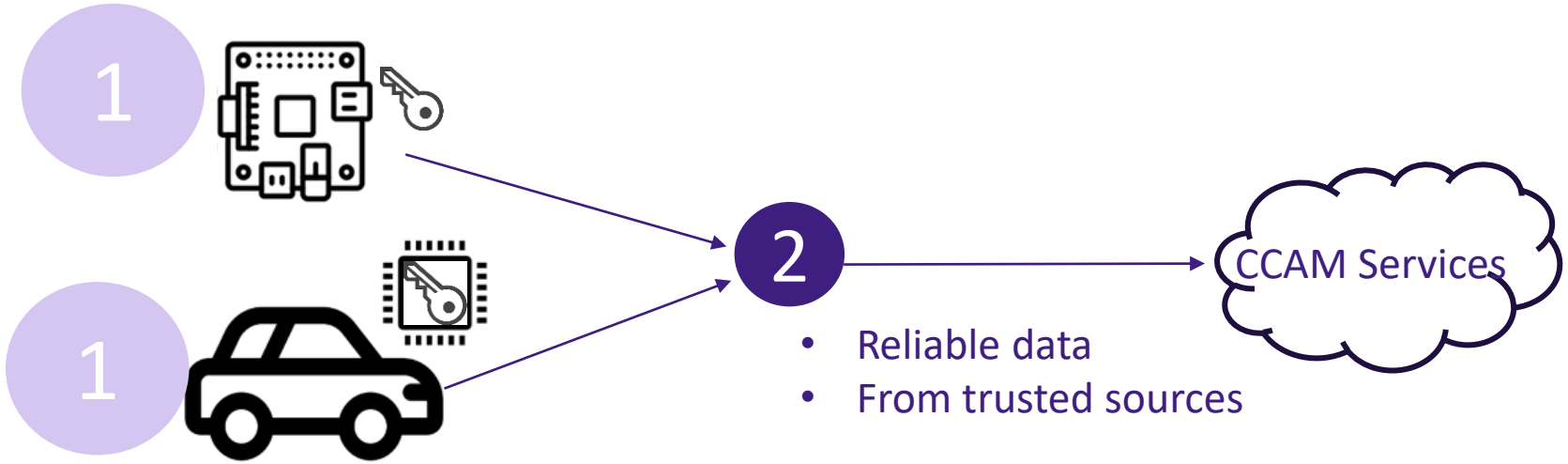
Data Fusion outcomes



- Algorithms will rely on higher truthfulness data
- In UC4, VIMA outputs (IVIM CAV indication, DENM warnings) will deliver information with higher:
  - Probability of being certain
  - Precision (in the case of positioning)

Conclusion

- **Trust and Truthfulness in podium are reached with strategies:**
  - **Integrity**
  - **Data fusion redundancy-assestment**



Thank you!

PoDIUM

Co-funded by
the European Union

@PoDIUM_EU

PoDIUM Project

podium-project.eu