ETSI
The Standards People

Security Conference

# Road-Map Towards  Dynamic Trust Assurances for Safety and Security Convergence in Safety-Critical Systems


Presented by: Francesca Bassi

SystemX
INSTITUT DE RECHERCHE TECHNOLOGIQUE


19/10/2023

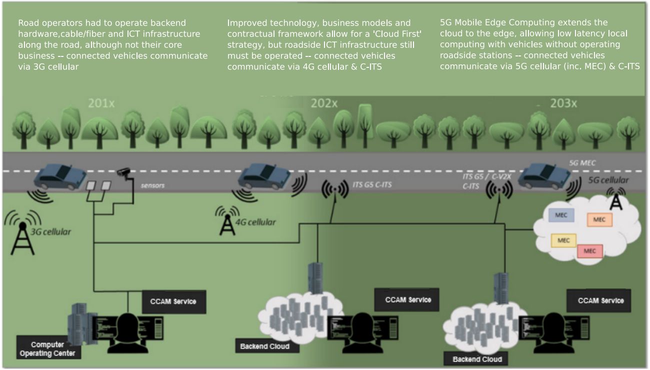
# CONNECT

- Continuous and Efficient Cooperative Trust Management for Resilient CCAM
- Cooperative, Connected and Autonomous Mobility

Funded by the European Union

Funded by the European Union under grant agreement no. 101069688. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

# MEC support for CCAM services




Source: based on Ertico

## 5G & Mobile Edge Computing

- 5G provides URLL communications
- MEC close to the service user
- → Low latency local computing
- → Support for safety-critical CCAM services

## Service example: platooning

- Automated highway corridors
- Platoon remotely managed by the MEC

# MEC support for CCAM services: challenges

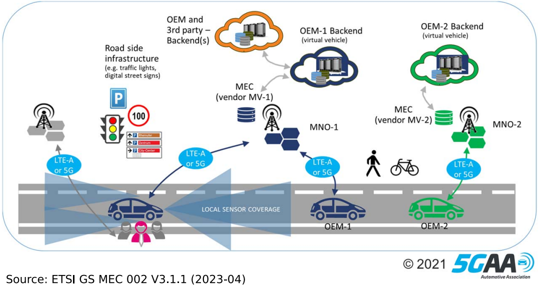


Complex system

- Multi OEMs
- Multi MNOs
- Multi service suppliers

→ Heterogeneous data sources, distinct security domains

→ Impact on the system's security




Source: ETSI GS MEC 002 V3.1.1 (2023-04)

# MEC support for CCAM services: challenges

## Complex system

- Multi OEMs
- Multi MNOs
- Multi service suppliers

→ Heterogeneous data sources, distinct security domains

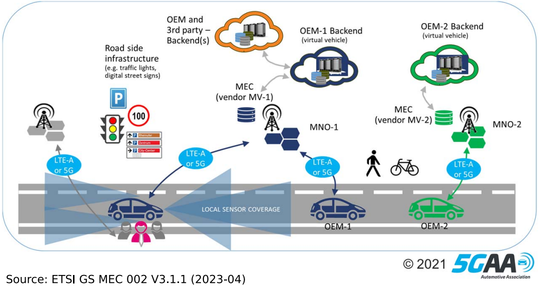
→ Impact on the system's security

## Challenge

- Collaborative data sharing between security domains
- Functional safety assurance

→ Need to dynamically assess trust to achieve resilience

→ Zero-trust principle



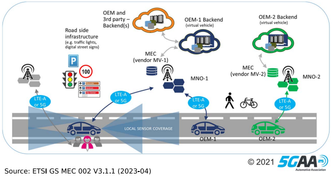

Source: ETSI GS MEC 002 V3.1.1 (2023-04)

## Platooning example

- Discovery of the MEC service (no shared trust domain)
- Handover between different MNOs / different vendors

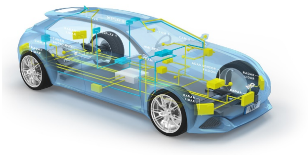
# Trust in CCAM applications

## Trust across the system

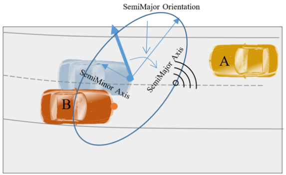



Source: ETSI GS MEC 002 V3.1.1 (2023-04)

## Trust within the vehicle

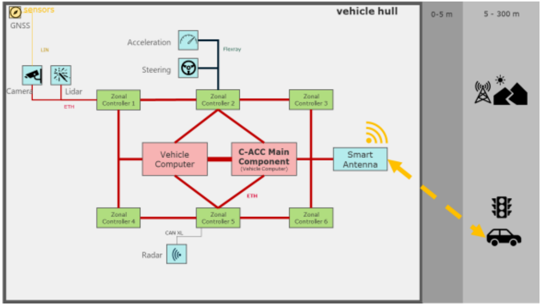


## Trust in the data




Dynamically assess trust between interacting components to achieve resilience

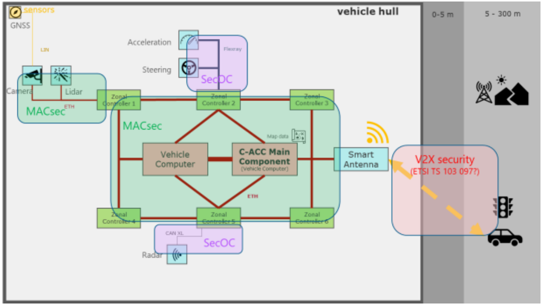
# Use case: trust needs in C-ACC




## C-ACC

- Cooperative - Adaptive Cruise Control

# Use case: trust needs in C-ACC




## C-ACC

- Cooperative - Adaptive Cruise Control

## Security features

- Bus between GNSS and camera unsecured
- Integrity protection on sub-networks only
- Integrity on dataflow through ZC1 non guaranteed

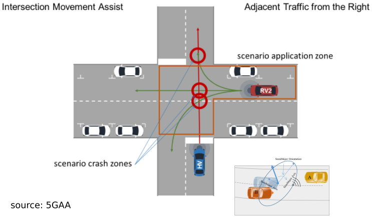
## Trust need example

- C-ACC component → camera
- Trust defined w.r.t. end-to-end data integrity

# Use case: trust needs in IMA

## Intersection Movement Assist

- Alert of collisions danger in the intersection
- Based on C-ITS messages (CAM and CPM)



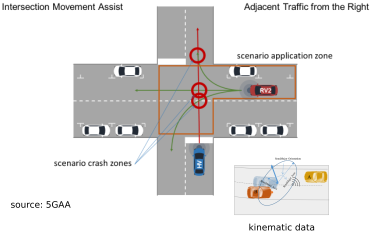

source: 5GAA

kinematic data

# Use case: trust needs in IMA

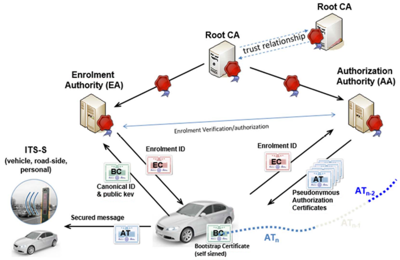
## Intersection Movement Assist

- Alert of collisions danger in the intersection
- Based on C-ITS messages (CAM and CPM)




source: 5GAA

## ETSI C-ITS PKI

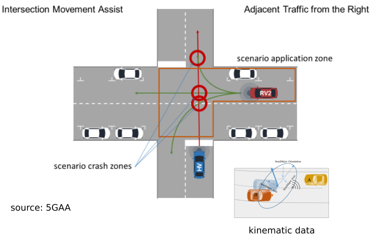



- Acces control & privacy
- Message: sender autenthication & integrity
- Misbehaviour: incorrect kinematic content in the message (intentional or not)

# Use case: trust needs in IMA

## Intersection Movement Assist

- Alert of collisions danger in the intersection
- Based on C-ITS messages (CAM and CPM)

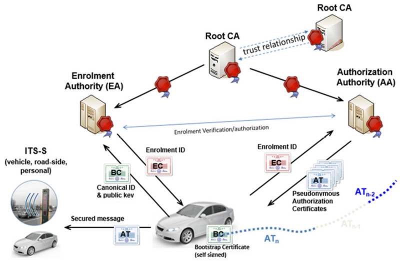



source: 5GAA

## Trust needs

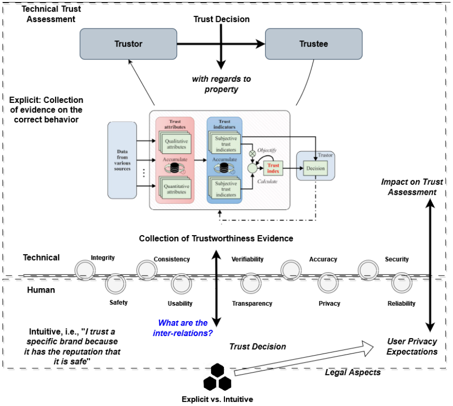
- IMA application → kinematic datapoint
- Trust defined w.r.t. datapoint correctness

## ETSI C-ITS PKI




- Acces control & privacy
- Message: sender autenthication & integrity
- Misbehaviour: incorrect kinematic content in the message (intentional or not)

# CONNECT: Trust modeling and assessment




## Trust relationship

- Between a trustor and a trustee, w.r.t. a property or task
- Allows to take a trust-related decision w.r.t. task

→ Expected behaviour of the trustee

## Trustworthiness

- Measure of the ability / compliance of the trustee

→ Technical assessment: based on the collection of trustworthiness evidence

→ User privacy expectations influence allowed evidence

## CONNECT's Trust Assessment Framework (TAF)

- Framework to continuously assess the collection of trust relatioships relative to a function (trust model)

horizon-connect.eu

# CONNECT: Trust enablers

## Zero-trust paradigm

- Never trust, always verify

## Trustworthiness evidence

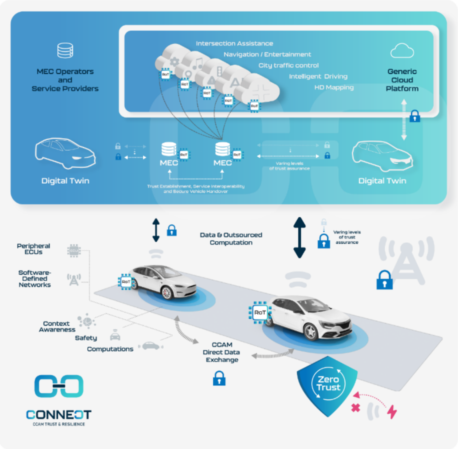
- Trustworthiness evidence collected by verifiable means
- Continuous verification of the configuration integrity of the underlying hw and instantiated sw stack
- Continuous verification of the of the execution state of the target system during runtime

→ Design a distributed Root of Trust supporting both the vehicle and the MEC for enabling trust

→ Leverage trustworthiness claims (as defined by IETF) for disclosing the attestation results as a trust source

## Do not breach privacy

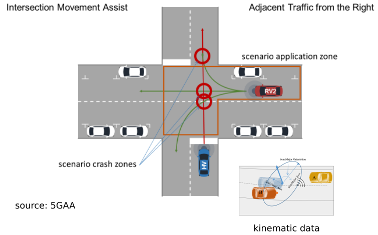
- Collecting evidence shall not break privacy profiles



# Exemple: IMA use case

## Trust needs

- IMA application → kinematic datapoint
- Trust defined w.r.t. datapoint correctness



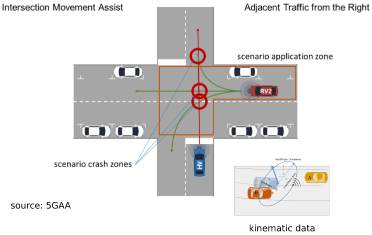

source: 5GAA

## What verifiable evidence?

# Exemple: IMA use case

## Trust needs

- IMA application → kinematic datapoint
- Trust defined w.r.t. datapoint correctness




## What verifiable evidence?

## Misbehaviour detection and reporting

- Local Misbehaviour Detection: detect incoherence in C-ITS messages (based on kinematic model)
- Misbehaviour Reporting: report misbehaviour detectors to backend

## Harmonised attributes (TCs)

- The vehicle verifies attestation evidence of integrity of internal components
- Trustworthiness claims (TCs) to the outside do not expose internal evidence
- Harmonized attributes are signed with anonymous credentials leveraging zero knowledge signatures

# Exemple: IMA use case (cont.)

## At the MEC

- TAF uses vehicle TCs and Misbehaviour Reports (MRs) as evidence for assessing trust in V2X-nodes
- The MEC provides trust levels of V2X-nodes as a service (V2X-Node Trustworthiness Message)

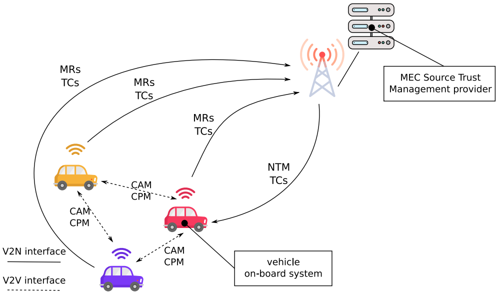
## At the vehicle

- TAF uses local misbehaviour detectors as evidence for assessing trust in data from V2X node
- TAF also uses trust level on the emitter V2X-node as evidence

## IMA application

- The IMA consumes only trusted kinematic data

→ It can rely on a more accurate view of the scene



# Conclusions



## Challenges in complex, multi-entity systems

- Increasing complexity has impact on the security of services

## Dynamic trust assurance

- Zero-trust principle
- Perform trust-based decisions grounded on verifiable evidence

→ Trust model: definition and assessment framework

→ Trustworthiness evidence: open questions

- What could be a base for mutual trust (e.g., quality of data, development process data, etc)?
- Which data is evidence, and on which basis (per function, per function class, per component?)
- Who are the stakeholders and what role do they have (e.g., standardization, regulation)?
- What is needed for acceptance and homologation?

CONNECT Grant Agreement No. 101069688

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@horizon-connect.eu

horizon-connect.eu

Funded by the European Union

Funded by the European Union under grant agreement no. 101069688. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.