CONNECT

CCAM TRUST & RESILIENCE

D1.3

Legal and Ethical Framework

Project number	101069688
Project acronym	CONNECT
Project title	Continuous and Efficient Cooperative Trust Management for Resilient CCAM
Start date of the project	1st September 2022
Duration	36 months
Call	HORIZON-CL5-2021-D6-01-04

Deliverable type	R
Deliverable reference number	D6-01-04 / D1.3 / V0.4
Work package contributing to the deliverable	WP1
Due date	Aug 2024 – M24
Actual submission date	2nd September 2024

Responsible organisation	UTWENTE
Editor	Adam Henschke
Dissemination level	PU
Revision	V0.4

Abstract	This deliverable presents the second and final version of the CONNECT Data Management Plan. In addition, the deliverable includes a roadmap definition as it pertains to the ethical and legal aspects of the Trust Assessment part, which plays a central role in CONNECT.
Keywords	DMP, research data, ethics, trust, trustworthiness

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

Document Revision History

Version	Date	Description of change	List of contributors
V0.1	09.07.2024	ToC created	Adam Henschke (UTWENTE), Lisa Burgstaller-Hochenwarter (TEC)
V0.2	02.08.2024	Inputs from technical partners collected in Chapter 2, draft of Chapter 4	Anna Angelogianni (UBITECH), Adam Henschke (UTWENTE),
V0.3	26.08.2024	Chapter 3 and Chapter 4 finalized	Adam Henschke (UTWENTE)
V0.4	02.09.2024	Chapter 2 finalized, internal review completed	Adam Henschke (UTWENTE), Anna Angelogianni, Thanassis Giannetsos (UBITECH)

Editor
Adam Henschke (UTWENTE)

Contributors
Lisa Burgstaller-Hochenwarter (TEC)
Anna Angelogianni (UBITECH)
Thanassis Giannetsos (UBITECH)
Chirag Arora (UTWENTE)

Disclaimer
The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

The scope of the present document is twofold: (i) to present the second and final version of the CONNECT Data Management Plan, offering the latest updates on the types of research data managed and processed by CONNECT, both in relation to the developed artifacts and the experimentation activities associated with the Use Cases, (ii) to elaborate on the roadmap established by CONNECT to integrate the legal and ethical dimensions into the trust assessment methodology, specifically tailored to the Connected and Cooperative Automated Mobility (CCAM) landscape. It shall be noted that the technical capabilities required for trust assessment in the context of CCAM have already been described in the deliverables of WP3. CONNECT differentiates from similar initiatives in the domain of trust assessment as it further addresses the legal and ethical aspects of such a framework. In this regard, this deliverable introduces the roadmap adopted for analysing these dimensions, with additional details to be provided in D2.2. Finally, it is important to mention that, in compliance with the Data Management policy, all the referenced research data are open source.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

This deliverable outlines the CONNECT Data Management Plan, presenting the outcome of T1.4 “Data Protection, Legal & Ethical Compliance”. The scope of the present document is twofold: (i) to present the second and final version of the CONNECT Data Management Plan, offering the latest updates on the types of research data managed and processed by CONNECT, both in relation to the developed artifacts and the experimentation activities associated with the Use Cases, (ii) to elaborate on the roadmap established by CONNECT to integrate the legal and ethical dimensions into the trust assessment methodology, specifically tailored to the Connected and Cooperative Automated Mobility (CCAM) landscape.

The roadmap introduced in this deliverable lays the foundation for analysing the legal and ethical dimensions of the Trust Assessment Framework (TAF). It introduces the trustworthiness principles outlined in the EU AI Act and contextualizes them within the CCAM domain. This initial mapping will be further developed in D2.2, where these principles will be more deeply integrated into CONNECT’s trust assessment methodology to ensure comprehensive coverage of ethical and legal considerations.

Chapter 3 of this deliverable provides a detailed analysis of the steps outlined in the roadmap, explaining how CONNECT will ensure that trustworthiness principles are effectively incorporated into the overall TAF, addressing dimensions beyond the purely technical. Additionally, to ensure that the functionalities offered by the TAF meet stakeholder needs, CONNECT has identified key questions for which feedback will be sought from the community. The results of this feedback process will be documented in D6.2.

Finally, it is important to underline that, in alignment with the Data Management policy, all referenced research data in this deliverable are open source, ensuring transparency and accessibility for further research and development efforts.

The aforementioned points are analysed in three chapters as follows:

- Chapter 2 provides an update of the project’s Data Management Plan (DMP) and the research datasets generated in the project;
- Chapter 3 outlines legal and ethical considerations, with a particular focus on relevant legislation and regulations, and describes the project’s planned engagement with stakeholders;
- Chapter 4 defines the concept of trust and trustworthiness and describes the envisioned roadmap that establishes the connection between ethics and trust.

Some conclusions are drawn in Chapter 5, while an Appendix at the end of the document showcases exemplary research datasets from the table in Chapter 2.

Chapter 2 Management of research data

In this chapter, an update of the project's Data Management Plan (DMP) is provided. In particular, a table shows the research datasets generated per partner for each technical component of the project.

2.1 Update of the DMP

In the Data Management Plan (D1.1) submitted in M06, the consortium described its approach towards research data management in the project. In particular, the data management life cycle for the data to be collected, processed and/or generated by CONNECT was outlined and particular attention was put to the FAIR data principle that makes research data findable, accessible, interoperable and re-usable. By means of a questionnaire, all technical and use case partners delivered information about the data that will be generated in the project, both as an outcome of the research innovations of CONNECT, and of the evaluation and benchmarking to be conducted in each of the three use cases. The result of the questionnaire was a preliminary list of datasets with information on characteristics like data type, format and management tools.

The outlined data management life cycle implemented in the first project year has worked efficiently so far. CONNECT has commenced the dissemination of this data as open source by means of open access scientific publications. The same approach will be applied for the results of the benchmarking once the evaluation activities are completed.

2.2 Research datasets per technical component

Now, after the first release of the CONNECT framework, an update of the datasets is provided for each technical component (see Table 1). All components are based on simulated data that are open-source and no specific restrictions are applied to this type of data.

Since the uses cases will be tested in a controlled environment, no real data will be generated out of them. Instead, they will produce synthetic data that will be made open-source.

All research data related to the technical components (see Table 1) will be published on the project's GitLab as well through open access scientific publications.

Some examples of CONNECT research datasets can be found in 0.

Table 1: CONNECT research datasets per technical component

CONNECT Activity	Type of data	Format	Management Tool	WP	Partner
Evaluation of CONNECT Trust Assessment Framework (TAF) in the context of the Use Cases	Simulation datasets capturing the trust models for IMA, C-ACC, SMTD Use Cases	Streams of time-stamped values, labelled (to differentiate the characteristics of each measurement) Text format (Log file)	Further processing can happen by means of any text-processing scripts or any statistics software.	WP3	UULM
Definition of the Trust Assessment methodology	Generated trust graphs enabling trust opinion calculation for trust models of varying complexity. As part of the fully full-fledged TAF, the TLEE will receive this input from the TAM component. The trust models will be generated by the TMM, and the numerical opinions for each trust relationship/edge of the graph will be calculated by the TSM.	The trust graphs are in .json format, but for debugging purposes, we generate also .gv and .gv.svg data formats of the trust networks. Also, for testing purposes we also store a .csv file that holds the values of the numerical opinions for each trust relationship/edge of the trust graphs.	No particular management tool needed. The graphs are generated with native go functions, and used as input to the TLEE.	WP3	HUAWEI
Definition of the Trust Assessment methodology	Logs showing transfer of state between local and remote TAF for synchronising the trust models as part of the Digital Twin (DT) TAF mode of operation	CSV or JSON containing at least timestamps and state data for the trust models	Spreadsheets Ad-hoc processing scripts	WP3	TRIALOG
Definition of the Trust Assessment methodology	Logs of requests from local TAF to remote TAF and their response, for synchronising the trust models as part of the DT-TAF mode of operation	CSV or JSON containing at least timestamps, type of request and response	Spreadsheets Ad-hoc processing scripts	WP3	TRIALOG

CONNECT Activity	Type of data	Format	Management Tool	WP	Partner
Definition of the Trust Assessment methodology	Performance metrics for Digital Twin synchronisation in terms of application and trust assessment task offloading	CSV or JSON containing comparison data for state convergence between local and remote TAF	Spreadsheets Ad-hoc processing scripts	WP3	TRIALOG
Definition of the Trust Assessment methodology	Threat Modelling and newly developed Risk Assessment methodology merging CVSS 3.1 and attack TARA	JSON	Git	WP3	UBI
Definition of the Trust Assessment methodology	Service metrics for RTL/ATL calculation	Streams of time-stamped values, labelled (to differentiate the characteristics of each measurement)	Git	WP3	DENSO
Definition of trust extensions for enabling trust assessment	Trusted Computing Base enablers for secure lifecycle management of connected cars (software update migration)	JSON	Intel SGX and Gramine acting as the underlying Root of Trust	WP4	INTEL
Definition of trust extensions for enabling trust assessment	Attestation enablers and software abstractions for supporting the self-issuance of security claims	Code written in C	Intel SGX and Gramine acting as the underlying Root of Trust	WP4	UBI
Definition of trust extensions for enabling trust assessment	Key management schemes	X509 key certificates for the CCAM PKI. For the TEEs keys will be generated by the TEE and the public keys made available to the other components in the system. Format TBD	PKI keys will be generated by scripts as part of the use case(s) For the TEEs the public keys will be provided to and managed by the IAM.	WP4	SURREY

CONNECT Activity	Type of data	Format	Management Tool	WP	Partner
	Service Metrics for capturing the communication between vehicle and MEC			WP5	ICCS
Definition of trust extensions for enabling trust assessment	ID & authentication management in the CCAM continuum	Attribute keys and monotone span program (MSP) data used for DLT access control The MSP data will be derived from access trees specifying which sets of attributes are necessary for access. The exact format TBD.	Programs to process the access tree and generate the MSP. Attribute keys will be generated by scripts and made available to the vehicles and other entities who should have access (i.e., OEMs).	WP5	SURREY
Evaluation of CONNECT Trust Assessment Framework (TAF) in the context of the Use Cases	CAM & CPM messages as well as CCAM functions in the context of the envisioned UCs (i.e., IMA)	Message traces of the V2X messages exchanged generated through the simulation framework Artery (for SystemX)	Wireshark or Tshark + any text-processing scripts.	WP6	SYSTEMX
Evaluation of CONNECT Trust Assessment Framework (TAF) in the context of the Use Cases	CAM & CPM messages as well as CCAM functions in the context of the envisioned UCs (i.e., SMTD)	Message traces of the V2X messages exchanged	Wireshark or Tshark + any text-processing scripts		CRF

CONNECT Activity	Type of data	Format	Management Tool	WP	Partner
Evaluation of CONNECT Trust Assessment Framework (TAF) in the context of the Use Cases	Mobility data as well as CCAM functions in the context of SMTD. V2X messages are extracted both from simulated vehicles and from the real equipped vehicle.	Message traces of the V2X messages exchanged	Wireshark or Tshark + any text-processing scripts. The simulated traces are produced with ms-van3t simulator (https://github.com/ms-van3t-devs/ms-van3t).		POLITO
Evaluation of CONNECT Trust Assessment Framework (TAF) in the context of the Use Cases	Simulated dataset for evaluating misbehaviour detection services in the context of IMA	Misbehavior Report and Extended Perception data + logging results of the IMA indicators in JSON or CSV format	Any script processing tool such as python	WP6	SYSTEMX
Evaluation of CONNECT Trust Assessment Framework (TAF) in the context of the Use Cases	Simulated vehicles' kinematic data. Produced internally by SUMO. Kinematic data may include speed, velocity, acceleration, and position of a simulated vehicles.	Streams of time-stamped values, labelled (to differentiate the characteristics of each measurement) in text format (log file)	SUMO	WP6	DENSO

Chapter 3 Legal and ethical considerations of CONNECT

In this chapter, CONNECT outlines the relevant legislation regarding the data produced and collected in the research, for the use case data and the engagement with stakeholders and users in WP6 and write about the plans for generating questionnaires that will be defined in D2.2 and put forward in D6.2 in the context of impact in WP6 (see task 6.5 description) incl. informed consent procedures to be applied. We point that there are two different aspects here: The first is concerned has to do with the relevant legislation on the management of the research data produced as part of the research and evaluation activities of CONNECT. The research data, including also those that stem from the evaluation of our use cases, is based on simulated and emulated environments, thus, they do no include any personally identifiable or information. The second aspect involves our testing and validation of CONNECT's work with key stakeholders. This core activity not only allows us to check if our findings are valid, but also for allowing CONNECT to achieve of the endmost goal of helping identify and develop a trust assessment methodology that can technically provide the necessary means for establishing trust that it also worthy of human trust.

3.1 Relevant regulations for research data

The primary regulations governing research data are derived from the General Data Protection Regulation (GDPR). CONNECT complies with these regulations by ensuring that no Personally Identifiable Information (PII) or sensitive data is collected during its research and evaluation activities. Instead of using real V2X messages, CONNECT leverages simulated messages that ensure the accurate representation of the required functionalities. Furthermore, alongside simulations, emulations and "hardware-in-the-loop" approaches are employed. This approach not only guarantees adherence to data protection regulations but also provides the necessary agility for conducting testing and evaluation activities across the various scenarios that are investigated and their distinct conditions.

In the specific scenarios under examination, V2X messages are used to assess the scalability of the Trust Assessment Framework (TAF) and to analyze their impact on the trust levels indicated by the TAF for a given service. Notably, even in the Slow-Moving vehicle Traffic Detection (SMTD) scenario, which is tested in a real test track by CRF and POLITO, the CAM and CPM messages used are simulated. This approach, based on simulated data, facilitates the comprehension of how stakeholders can potentially exploit these trust calculations to improve the trustworthiness and effectiveness of their services

The overarching objective of CONNECT is to establish a Trust Assessment methodology tailored to the unique needs of the CCAM environment. To this end, and as further discussed in the following chapter, CONNECT not only explores the technical aspects but also considers the social and ethical dimensions of trust. The goal is to interpret the interplay between these dimensions and their influence on end-user and stakeholder acceptance of such a framework. To address the social and ethical aspects of trust, CONNECT examines newly introduced standards and regulations. In particular, CONNECT leverages the EU AI Act, which outlines 7 key areas for trustworthy AI and employs them as a basis for determining the trustworthiness principles in the CCAM field. A thorough discussion of this roadmap can be found in Chapter 4.

3.2 Engagement with CCAM stakeholders

As part of its social and ethical analysis within the CCAM context, CONNECT engages with key stakeholders and expert groups. More specifically, among the aforementioned stakeholders and expert groups, OEMs (both Tier 1 and Tier 2 suppliers), security providers, and CCAM technology providers are included. CONNECT leveraging the extensive expertise and already established networks of its partners—including Tier 1 OEMs like DENSO and Tier 2 OEMs like CRF—and its advisory board, which includes carefully selected experts from industry leaders such as Toyota, Volkswagen, and Qualcomm. As part of CONNECT analysis tasks, it has been recognised that users including drivers, passengers, etc. are also an integral part of the stakeholder ecosystem focus will be given on engaging to the set of stakeholders that provide CCAM services and technologies as a starting point. This does not confine the impact of our findings since for both types of stakeholders there is the same core expectation that delineates the characteristics that deem an automotive system worthy of human trust (i.e., to travel safely from point A to point B). Through these interactions that include targeted interviews, the project aims to assess how these stakeholders might benefit from the proposed Trust Assessment Framework. The following table summarizes the involved stakeholders and outlines their relevance to the project.

Table 2: Stakeholders and their relevance to CONNECT

Type of stakeholder	Relevance
Tier 1 OEM (i.e., DENSO, Bosch)	Tier 1 OEMs are focused on delivering CCAM services that rely on accurately determining whether data is trustworthy or untrustworthy. As such, they are interested in the Trust Assessment Framework (TAF) to evaluate and characterize the trust level of a given service.
Tier 2 OEM (i.e., CRF, Toyota, Volkswagen)	Tier 2 OEMs interested in the elevation of trust from the in-vehicle components towards the characterisation of trust for the entire vehicle.
Security Service Providers (i.e., Intel)	Interested in the deployment of Trusted Computing capabilities for enabling the trust assessment.
CCAM Technology Provider (i.e., Qualcomm)	Interested how the trust assessment can be considered for the entire CCAM continuum including the MEC.

Chapter 4 CONNECT Roadmap Towards Analysing Ethical & Legal Dimensions of Trust in CCAM Environments

In this chapter, we outline the concept of trust and its explanation to stakeholders like users or service providers. The roadmap sets out the context in which we examine the dimensions and determinants that affect the trust that humans can understand, so that a system like CONNECT can offer ways of conceptualising trust beyond the technical dimension that has currently been investigated in the technical activities as documented in D3.1 and D3.2. We want to develop methods that allow us to understand the interplay between how trust is expressed in technical terms and how this is translated by humans – e.g., that a system is worthy of human trust as this has a direct impact on the user adoption of CCAM technologies. The first step in this endeavour is the definition of trust and trustworthiness as a general concept (following the standards) and its concretization in the context of CCAM.

The question here revolves around the ethical and social dimensions of trust, and their interpretation by the users. This is a different set of considerations of trust than that of the technical components - this is in contrast to the quantification of trust as has been described in CONNECT's technical deliverables. This chapter puts forth the activities and steps that CONNECT has identified as part of a methodology to be followed to that all trust enablers that been designed in CONNECT are also ethical, i.e., privacy-preserving, and worthy of human trust. We identify the key areas that capture the social/ethical dimensions of trust as they apply to CCAM. These conceptual and ethical discussions set the foundations to enable key stakeholders to identify what is valuable within the system. There is an implicit interplay between what a system can achieve technically (in a trustworthy manner) and how this relates to what is valued by stakeholders. D1.3 presents a set of steps make these relationships explicit.

In what follows we set out the roadmap for how we make these relations explicit, and in D2.2 we will provide specific details on how to do this in practice.

4.1 Definitions of trust and trustworthiness

The main question we are seeking to answer here is, when we discuss trust (generally) what are we talking about? For the purposes of CONNECT, we also note a distinction between a general concept of trust, and a general concept of trustworthiness. While trust, the judgement or assertion that some person, component, or process can be relied upon, is essential to CONNECT, given the technical focus of CONNECT, we are more often working on whether a component or process is worthy of trust, can it be relied upon?

For specific trust relations, and for particular expectations about whether a component or process is worthy of trust, we have developed general definitions of trust and trustworthiness. In CONNECT we start from a general definition of trust and trustworthiness (rooted to the vocabulary already identified in the ISO and ITU-T standards) so as to delineate a concrete instantiation of trust and trustworthiness in the context of CCAM. This is the first important step that is necessary for guiding the entire ethical analysis. Thus, in this chapter we start by summarizing this general definition of trust based on which the CCAM-centered trust and trustworthiness was defined in the context of D3. The intention here is to use CONNECT to demonstrate not only that our components and processes are worthy of trust, but also that the work produced here can be generalised – by offering a conceptual analyses of trust and trustworthiness, we are able to offer a set of analytic tools that can be used and applied to the new generation of Systems-of-Systems with a high degree of automation (connected cars and autonomous vehicles) leveraging a wider set of applications based on artificial intelligence.

When conceptualising trust, we must first be clear what we are talking about with regards to trust, and second, we must clarify how it is a concept distinct from, but related to, trustworthiness. The

basic distinction between the two is that trust is concerned with the judgment made by a trustor about the subject that they are trusting. In contrast, trustworthiness is concerned with whether a subject of trust is worthy of that trust. A driver of a connected vehicle will make a judgment about whether they trust that vehicle. This is distinct from whether the vehicle is should be, or is, worthy of that trust.

Following this distinction, we offer the **general definition of trust (GDoT)**. This definition is intended to be general, and generalisable. It is developed in such a way as to be adapted and specified to specific applications and particular trust relationships. In earlier CONNECT deliverables we have drawn from the GDoT to give a definition for CCAM that is specific for the context of CCAM applications (See D2.1 and D3.1). By developing this general definition, we are able to give a solid conceptual foundation for the following roadmap.

The GDoT is given as :

$T_{A,B}$ – A relies on B to exhibit trust R(X) in Context (C) to a degree (D) given a warrant (W)

The GDoT describes a trust relation between A (trustor) and B (trustee), given at $T_{A,B}$.

This trust relation between A and B signifies that A is trusting B. Our driver is trusting their connected vehicle.

This is quite general, and so we need to say more about what A is trusting the vehicle to do. R needs to conform to A's expectations regarding the outcome (performance), procedure (or process), and purpose. Such expectations can be predictive and/or normative (where A has the attitude that B *should* exhibit R(x) along such lines. We can simplify this by stating that A expects B to perform the goal X – A relies on B to perform X, or A relies on B to exhibit behaviour - R(X) Our driver trusts their connected vehicle to drive safely.

We need further detail on what this 'safely' means, we have to give some clarity to the context in which A is trusting B. We need to say something like the driver of our Connected vehicle is relying on the vehicle to safely navigate the vehicle on a road, in traffic, in a way that preserves the quality of the data, the driver's privacy and so on. The action, X, that A is trusting B to is going to occur in a particular context, C. This general definition is designed to capture all important dimensions for navigating the type of evidence that need to be monitored for allowing A to make a decision on whether its trusting B in a specific context. This means that all of our activities can extend beyond the specifics explored in CONNECT, such that we can achieve an overarching trust assessment methodology.

Next, we have to recognize that trust comes in degrees – Trust judgments will be affected by uncertainty and disbelief. When considering the way people trust each other, A will typically trust B more or less, given a range of contingent features and experiences. A might wholly trust B to navigate through an intersection safely, but might only partially trust B to secure their private information. In some cases, trust might not be considered in degrees but in a binary fashion. For our use of trust within CONNECT, trust is treated in this way (See D2.1 and D3.1). However, for other considerations, trust may be partial.

Underpinning all of these elements of A's trust judgment about B is the reasons, evidence, or data that A has for trusting B. Ideally, A has good reasons to trust B to navigate the intersection safely, or might have good reasons to only partially allow B to handle their information securely. Warrant is a reference to the reasons, evidence, or data why A might or might not trust B. For instance, their vehicle might be produced by a company that has never had a crash with any vehicle going through an intersection. Or, the company might have suffered some cybersecurity failures, indicating that they cannot properly secure the data of their vehicles. **The main technical objective of CONNECT is to explore way of providing reasons, evidence, or data, that give a component, user, or other stakeholder that warrant**.

So, using the GDoT, we might say that when describing the trust relation between a driver and a connected vehicle ($T_{A,B}$), we are saying that the Driver (A) relies on their vehicle (B) to reliably exhibit safe navigation (R(X)) through an intersection (C) completely (D) given that their vehicle has never had a crash while navigating intersections (W).

Or, we might say that when describing the trust relation between a driver and a connected vehicle ($T_{A,B}$), we are saying that the Driver (A) relies on their vehicle (B) to partially secure information (R(X))

about travel history (C) to a given degree (D) given that the company has had cybersecurity failures (W).

This GDoT is also applicable to component trust relations. A does not have to be a human driver, and B does not have to be the complete vehicle. We might also say that when describing the edge computing trust relation between a vehicle and the intersection cloud management system ($T_{A,B}$), we are saying that the vehicle (A) relies on the intersection (B) to reliably collect and communicate (R(X)) information about vehicle movement (C) completely (D) given that all vehicles in the given intersection are providing accurate information about their movement through the intersection (W).

We note here how these trust relations depend on W, that the trust judgments being formed by A about B are accurate. This leads us to reflect on the notion of trustworthiness – what is sufficient reason, evidence, or data to justify A trusting B? When building trust into complex systems like CCAM, it is not enough to simply say or assess if A trusts B, we must also ask if B is *worthy* of A's trust. To this end, we must also reformulate the GDoT to be a general definition of trustworthiness, given here as GDoTW.

$Tw_{B,A}$ – A has W that they can rely on B to exhibit behaviour R(X) in Context C to Degree D.

As before, GDoTW is concerned with a trust relation between A and B, in which A has warrant to rely on B to exhibit particular behaviour in a specific context to a particular degree. This GDoTW repeats the same information at the GDoT, however, it is now focused on whether B is worthy of that trust. For instance, a driver might trust their vehicle to be safe, but it may not be able to navigate an intersection without significant risk of crashing. A may trust B, but B is not worthy of that trust.

To illustrate why a distinction between GDoTW and GDoT is needed, we can consider a case where A trusts B, but B is not worthy of that trust. Consider that A trusts the vehicle B to handle their personal information securely, given that B is not known to have suffered any cybersecurity failures. A is forming a trust judgment about B. However, what if the company that provides cybersecurity to all B vehicles has suffered numerous cybersecurity attacks, and the information that they store is not, and has never been secure. Here, B should not be considered worthy of A's trust. We can also consider a contrasting case where A does not trust B, but B is in fact worthy of that trust. Consider now that A does *not* trust B navigate an intersection safely, and always takes control over B as they move through the intersection, despite the fact that all models of B are 100% reliable to navigate these intersections safely. Here, we have a problematic judgment of B's trustworthiness, where is not trusting B, despite the fact that they should be.

Thus, any considerations about trust and CCAM needs to consider both trust relations and trustworthiness relations. For some purposes, it might be more important to focus on A and GDoT, while for other purposes, it might be more important to focus on B and GDoTW.

Having provided these general definitions of trust and trustworthiness, we suggest that the process for understanding trust relations and the trustworthiness of a trustee can be generalized. The process is as detailed above – *in order to describe a trust relation between a trustor and trustee, one should identity who/what A and B are, the goal that A is expecting B to meet, the context in which the goal is expected to occur, the degrees of trust that A wants and needs from B, and the reasons, evidence, or data that A needs to make a warranted trust assessment*. Similarly, when asking if the trustee is worthy of the trustor's trust, we need to detail the goal and context in which B is expected to operate, the degree of trust that B needs to meet in order for that goal to be met, and importantly, what reasons, evidence, or data that B can provide to A to ensure that B is worthy of A's trust or not.

Figure 1 shows how the GDoT and GDoTW relate to wider considerations of what counts as being trustworthy, and how they feed into the three Use Cases. The Seven Key Trustworthiness Principles come from the EU High Level Ethics Group (HLEG) and The Assessment List for Trustworthy Artificial Intelligence (ALTAI) (Fernandez Llorca & Gomez, 2021).[1] The HLEG engaged in a deep anaylsis of 350+ experts in AI and related technologies, and identified Seven Key Areas in which AI must meet in order to be trustworthy. They are:

1. Human Agency and Oversight
2. Technical Robustness and Safety
3. Privacy and Data Governance
4. Transparency
5. Diversity, Non-Discrimination and Fairness
6. Societal and Environmental Well-Being
7. Accountability

D2.2 involves an extended analysis of each of the Seven Key Areas, and adapts the ALTAI for the CCAM context, with particular attention to CONNECT and its use cases.

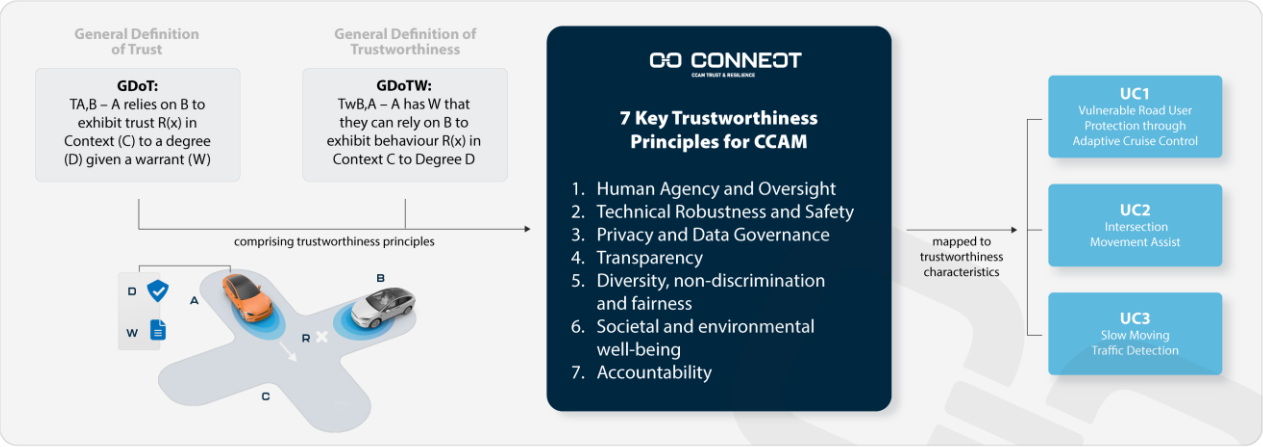


Figure 1: Representation of trust, trustworthiness and relations to key trustworthiness principles (taken from the ALTAI), and to CONNECT use cases.

In D2.2 we specify in detail how the GDoT and GDoTW were developed, where the different conceptual elements came from, and how CONNECT engages in specifying the GDoT and GDoTW in design and practice in reference to the HLEG Seven Key Trustworthniess Principles for AU, and giving particular consideration of how trustworthiness applies to CONNECT's three use cases; intersection management, dynamic cruise control, and information security/intrusion detection.

4.2 Connection between Ethics and Trust

Having clarified the related notions of trust and trustworthiness, we are now in a position to elaborate how ethics and trust are related in CONNECT, and in informationally mediated cyber-physical systems more generally. The basic idea here is that, in order for something to be trustworthy, it must meet some particular criteria. For instance, consider if someone were to ask if they could trust a connected vehicle, and the answer was, yes, it is safe. Safety here is providing a specific criterion by which the connected vehicle is deemed trustworthy, thus, the person can and should trust the connected vehicle. Likewise, consider if someone were to ask if they could trust a babysitter, and the answer is yes, they are safe. Safety here suggests more than just mere competence, it suggests that the babysitter not only knows what they are knowing, and has the capacity to do their job, but

[1] See https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html

also suggests that they will not put the child at risk. While more complicated, if the answer is yes, the person can and should trust the babysitter. In this second case, however, there is more that is needed in order for the person to trust the babysitter. Likewise, in cyber-physical systems like CCAM systems, the particular features that are being trusted are complicated and pose particular and collective challenges.

In CONNECT, we consider that there are criteria that CCAM must meet in order to be worthy of trust

Can Vehicle B navigate intersection safely?

Is Vehicle B worthy of the trust of other vehicles in the intersection, with regard to moving safely through the intersection?

Can Vehicle B engage in adaptive cruise control safely?

Is Vehicle B worthy of the trust of other vehicles on the road, with regard to moving maintaining safe traveling distances on the road?

Can Vehicle B produce/communicate information accurately?

Is the information produced and/or communicated by Vehicle B accurate, free from external interference?

In order to determine if a CCAM can be trusted or not, CONNECT has outlined a four step roadmap, Figure 2, below.

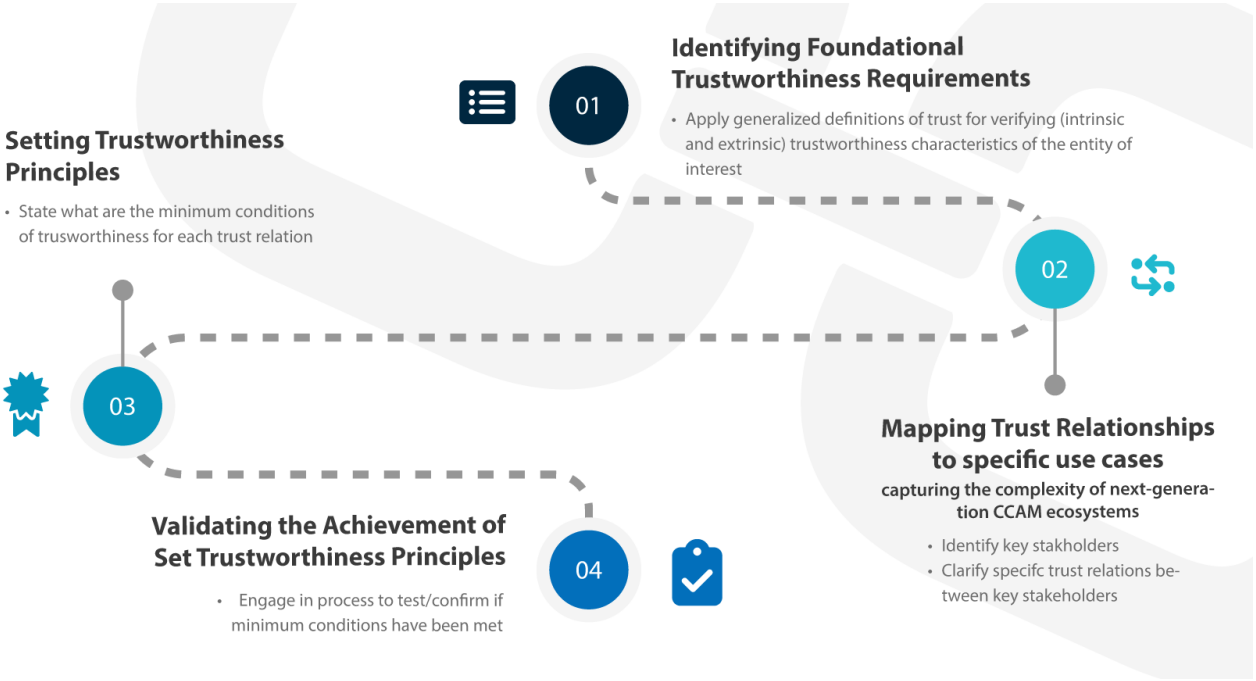


Figure 2: Roadmap for understanding, mapping, setting, and ensuring trust relations in CCAM

Step 1 is concerned with identifying the broad requirements of a system's trustworthiness. The first step in the roadmap is to take the GDoT and GDoTW and apply them to the particular system under consideration. As outlined in Section 4.1, the specific conditions of a trust relationship between trustor and trustee must be given. A and B must be identified, A's goal that B is expected to meet must be stated, in the specific context of expectation, with clarity given on the degrees of trust that A wants and needs of B, with the reasons, evidence, or data that A needs to make a warranted trust assessment. Similarly, when asking if B is worthy of the A's trust, we need to detail the goal and context in which B is expected to operate, the degree of trust that B needs to meet in order for that goal to be met, and importantly, what reasons, evidence, or data that B can provide to A to ensure that B is worthy of A's trust or not.

Step 2 is then concerned with mapping the trust relationships that arise between all trustors and trustees in the given system. Here, A and B might in fact have a range of different trust relationships. B might be expected to do X, Y, and Z. Or B might be expected to do Z, but in Context 1, Context 2, and Context 3. Similarly, given the particular system, there is likely to be a range of different stakeholders, so we would need to identify all the relevant stakeholders in a given trust network. Thus, A might need to trust B, C, and D. While B might need to trust E, F, and G, and C might need to trust H, I, and J, and so on. Following the GDoT and GDoTW, each of these stakeholder relationships need to be specified, such that it is clear what each trustor is expecting of each trustee, in which context(s), to what degree, and what reasons, evidence, and data are needed.

Steps 1 and 2 are going to be engaged through an iterative process, in which high level GDoT and GDoTW details are given, then stakeholders are identified, then more specific GDoT and GDoTW are given, perhaps leading to more stakeholder identification, and so on. The desired outcome is for a comprehensive map of the trust relationships between all the relevant stakeholders, who they are trusting to do what, and what those trust expectations, contexts, degrees, and warrants require.

Step 3 is concerned with setting the standards for what counts as a trustworthy relationship. For instance, if someone were to ask if a connected vehicle is safe, then there needs to be some standard – or set of standards – by which the notion of safe is given and clarified. Importantly, these standards are likely going to be something external or distinct from both the trustor and trustee. This goes back the importance of marking the distinction between trust and trustworthiness. By simply considering trust, the trustee might say that their car, or their babysitter is safe, and the trustor might believe them. But this does not actually say anything about whether the car or babysitter is actually safe.

Step 3 establishes the link between trust and ethics, whereby ethics is concerned with setting some standards about what *ought* to be considered worthy of trust. For now, we point to an approach in ethics, standards, and trustworthiness that CONNECT is adapting CCAM – D.2.2 takes the HLEG work and the ALTAI, and gives extended analysis of each of the Seven Key Areas, and adapts them for the CCAM, with particular attention to CONNECT and its use cases.

We note here first that the HLEG and ALTAI were specifically for AI, and CONNECT is not strictly bound to AI considerations. However, the core ethical values identified in the Seven Key Areas are highly relevant to CONNECT and to CCAM more generally. The Seven Key Areas must be adapted to CONNECT in order to ensure applicability. Second, as detailed in D2.2, as we move from Key Area 1 out to Key Area 7, the values become more generalised, and the adaption also needs to become more general. That is, the conditions relating to Human Agency and Oversight, Technological Robustness and Safety are much more easily translatable to specific engineering requirements and existing standards, whereas Privacy and Data Governance, and Transparency are technical features that are understood by reference to existing law, legislation, and policy, while Diversity, Non-Discrimination and Fairness, Societal and Environmental Well-Being, and Accountability are applicable to CCAM more generally than just CONNECT, and must also be understood by reference to existing law, legislation, policy, as well as emerging and evolving social norms.

Step 4 is the final part of the roadmap, in which the first three steps are validated and tested. As part of CONNECT WP6, we will is presenting the specific instructions for Steps 1-3, and the adaptations of the ALTAI to OEMs, automotive vendors, and security service providers. Step 4 is a way to validate the process, and test the specific questions and responses with a vital range of stakeholders, to tighten and improve the trust method in practice. At the end of the project, we will have a specified trust methodology which can be applied equally to CONNECT, to other CCAM, to autonomous vehicles, and to cyber-physical systems more generally.

Step 1 has been completed as detailed in D2.1 and D3.1. Step 2 has also been completed by mapping the trust relationships in the context of our use cases that capture CCAM services of mixed safety-criticality. We have also captured the relationships across the entire CCAM continuum – starting from considering the relationships between components within a vehicle to V2C and V2E relationships including also the integration of the MEC. As part of D6, we going to validate our findings/hypotheses through interviews and engaging with the identified stakeholders listed in Chapter 3.

Chapter 5 Summary and Conclusion

The present document elaborated on the final version of the CONNECT Data Management Plan, demonstrating the project's approach to managing and processing research data, either regarding the artefacts or in terms of the evaluation activities. Although this represents the final iteration of the plan, it is a living document that will evolve. As evaluation activities progress and with the introduction of the second iteration of the CONNECT framework, updates may be necessary to enhance the accuracy and management of all data types in line with ongoing advancements. The roadmap as outlined in this deliverable has been initiated, with the next steps clearly identified to further advance CONNECT's objectives. CONNECT is pioneering in the field of trust assessment for CCAM, distinguishing itself by integrating technical, ethical, and legal considerations into a unified framework.

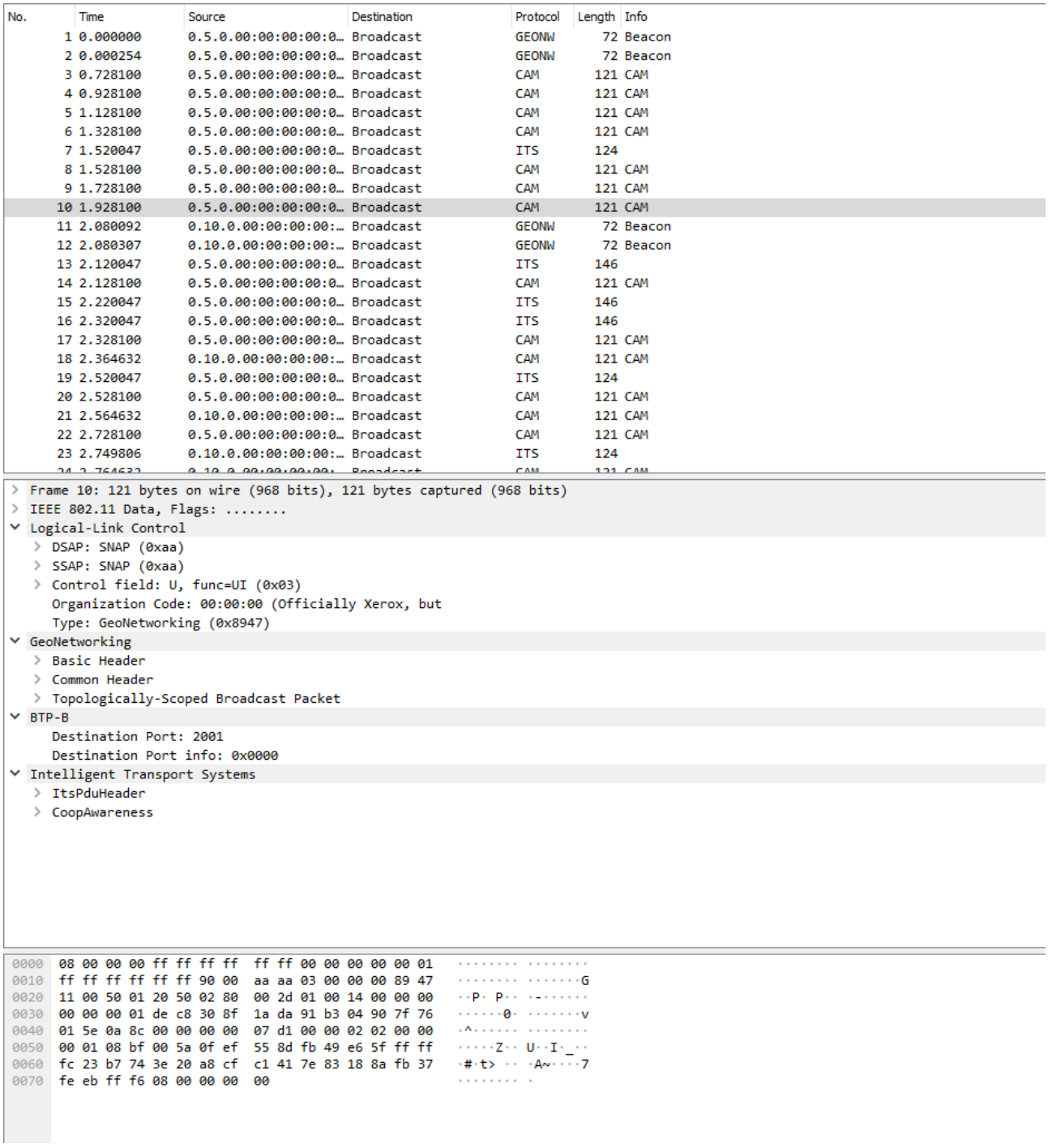
Further insights and detailed elaborations on these efforts will be provided in upcoming deliverables, specifically D2.2, which will delve deeper into the integration of trustworthiness principles, and D6.1, which will document the stakeholder feedback process and its impact on the Trust Assessment Framework. Through these continued efforts, CONNECT aims to establish a novel and widely accepted framework for trust assessment in the CCAM domain, ensuring broad acceptance and effectiveness within the community.

Chapter 6 List of Abbreviations

Abbreviation	Translation
CAM	Cooperative Awareness Message
CPM	Collective Perception Message
DMP	Data Management Plan
DoA	Description of Action
FAIR	Findable, Accessible, Interoperable, and Re-usable
GDPR	General Data Protection Regulation
MEC	Mobile Edge Computing
R&D	Research and Development
TCB	Trusted Computing Base

Appendix A: Examples of CONNECT research datasets

7.1 CAM/CPM PCAP example for UC3



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.5.0.00:00:00:00:0…	Broadcast	GEONW	72	Beacon
2	0.000254	0.5.0.00:00:00:00:0…	Broadcast	GEONW	72	Beacon
3	0.728100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
4	0.928100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
5	1.128100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
6	1.328100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
7	1.520047	0.5.0.00:00:00:00:0…	Broadcast	ITS	124	
8	1.528100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
9	1.728100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
10	1.928100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
11	2.080092	0.10.0.00:00:00:00:…	Broadcast	GEONW	72	Beacon
12	2.080307	0.10.0.00:00:00:00:…	Broadcast	GEONW	72	Beacon
13	2.120047	0.5.0.00:00:00:00:0…	Broadcast	ITS	146	
14	2.128100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
15	2.220047	0.5.0.00:00:00:00:0…	Broadcast	ITS	146	
16	2.320047	0.5.0.00:00:00:00:0…	Broadcast	ITS	146	
17	2.328100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
18	2.364632	0.10.0.00:00:00:00:…	Broadcast	CAM	121	CAM
19	2.520047	0.5.0.00:00:00:00:0…	Broadcast	ITS	124	
20	2.528100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
21	2.564632	0.10.0.00:00:00:00:…	Broadcast	CAM	121	CAM
22	2.728100	0.5.0.00:00:00:00:0…	Broadcast	CAM	121	CAM
23	2.749806	0.10.0.00:00:00:00:…	Broadcast	ITS	124	

```
> Frame 10: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
> IEEE 802.11 Data, Flags: ........
v Logical-Link Control
  > DSAP: SNAP (0xaa)
  > SSAP: SNAP (0xaa)
  > Control field: U, func=UI (0x03)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: GeoNetworking (0x8947)
v GeoNetworking
  > Basic Header
  > Common Header
  > Topologically-Scoped Broadcast Packet
v BTP-B
    Destination Port: 2001
    Destination Port info: 0x0000
v Intelligent Transport Systems
  > ItsPduHeader
  > CoopAwareness
```

```
0000  08 00 00 00 ff ff ff ff  ff ff 00 00 00 00 00 01   ........ ........
0010  ff ff ff ff ff ff 90 00  aa aa 03 00 00 00 89 47   ........ .......G
0020  11 00 50 01 20 50 02 80  00 2d 01 00 14 00 00 00   ··P· P·· ·-......
0030  00 00 00 01 de c8 30 8f  1a da 91 b3 04 90 7f 76   ......0· .......v
0040  01 5e 0a 8c 00 00 00 00  07 d1 00 00 02 02 00 00   ·^...... ........
0050  00 01 08 bf 00 5a 0f ef  55 8d fb 49 e6 5f ff ff   .....Z·· U··I·_··
0060  fc 23 b7 74 3e 20 a8 cf  c1 41 7e 83 18 8a fb 37   ·#·t> ·· ·A~····7
0070  fe eb ff f6 08 00 00 00  00                       ........ ·
```

7.2 CPM JSON example for UC1


```
{
   "sourceId":19,
   "referenceTime":444042959821,
   "longitude":2.197544,
   "latitude":48.712710,
   "semiMajorConfidence":4095,
```

```
   "semiMinorConfidence":4095,
   "semiMajorOrientation":3601,
   "orientationAngle":2783,
   "orientationAngleConfidence":127,
   "PerceivedObjectContainer":{
      "numberOfPerceivedObjects":2,
      "objects":[
         {
            "objectId":162,
            "measurementDeltaTime":21,
            "position_xCoordinate":-1191,
            "position_xCoordinateConfidence":4096,
            "position_yCoordinate":-139,
            "position_yCoordinateConfidence":4096,
            "velocityMagnitudeValue":125,
            "velocityMagnitudeValueConfidence":127,
            "velocityDirection":3497,
            "velocityDirectionConfidence":127,
            "accelerationMagnitudeValue":45,
            "accelerationMagnitudeValueConfidence":102,
            "accelerationDirection":1697,
            "accelerationDirectionConfidence":127,
            "zAngularVelocity":0,
            "zAngularVelocityConfidence":7,
            "zAngle":3497,
            "zAngleConfidence":127
         },
         {
            "objectId":806,
            "measurementDeltaTime":21,
            "position_xCoordinate":-8129,
            "position_xCoordinateConfidence":4096,
            "position_yCoordinate":1125,
            "position_yCoordinateConfidence":4096,
            "velocityMagnitudeValue":831,
            "velocityMagnitudeValueConfidence":127,
            "velocityDirection":3497,
            "velocityDirectionConfidence":127,
            "accelerationMagnitudeValue":2,
            "accelerationMagnitudeValueConfidence":102,
            "accelerationDirection":3497,
            "accelerationDirectionConfidence":127,
            "zAngularVelocity":0,
            "zAngularVelocityConfidence":7,
            "zAngle":3497,
            "zAngleConfidence":127
         }
      ]
   }
}
```


7.3 Misbehaviour Report JSON File Example


```
"CPM_REPORT":{

                "generationTime": 4158997360759,
                "reporterPseudoId": 1877275224,
                "reporterArteryId": 1310,
                "version": 1,
                "observationlocation":{
                        "x": 2138.765976,
                        "y": 981.058923
```

```
		},
		"content":{
			"observationSet":[
				{
					"targetId": 376,
					"check": 1
				}
			],
			"V2XPduEvidence":
				{
					"sourceId": 1877275183,
					"referenceTime": 404042941589
				}
		}
}
```

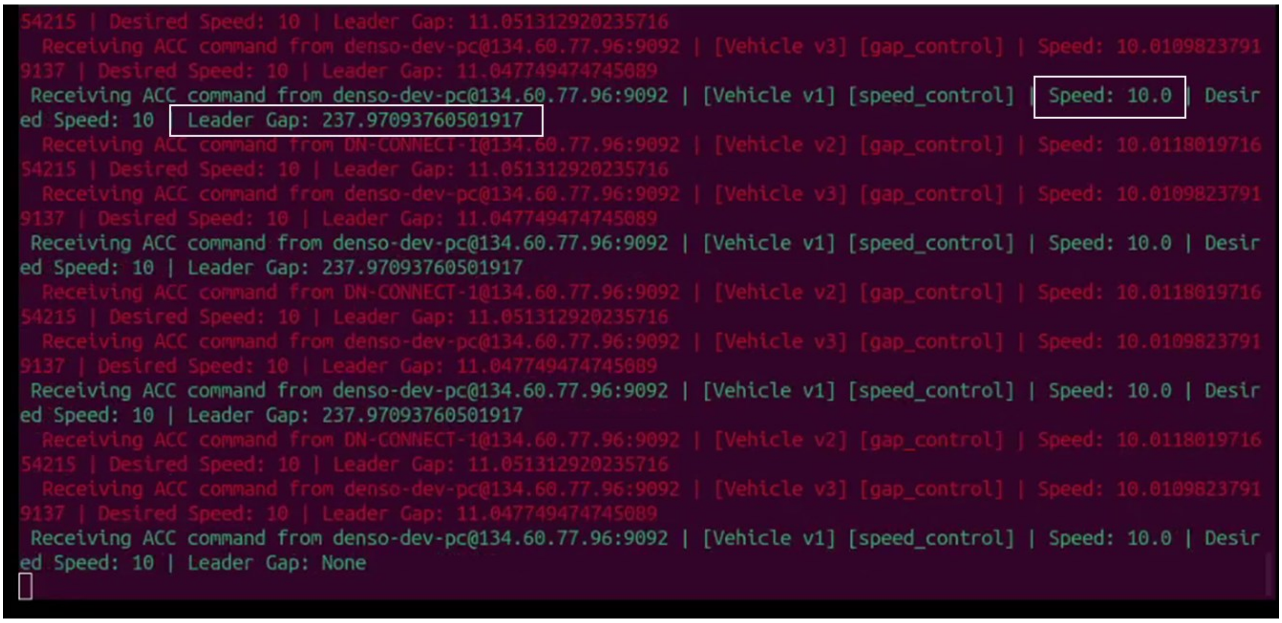

7.4 Extended Perception JSON file Example


```
{
		"timestamp": 50.174875313975,
		"myStationId": 805,
		"mySumoId": "a25",
		"Xegosumoposition": 1707.316322,
		"Yegosumoposition": 465.792799,
		"longitude": 2.195563,
		"latitude": 48.712903,
		"longspeed": 0.256010,
		"longacceleration": 2.568396,
		"orientationangle": 1003.000000,
		"ExtendedPerceivedObjects":[
			{
				"PerceivedObjectID": 18,
				"SumoPerceivedObjectID": "a1",
				"LastUpdateTime": 50.146000,
				"Observer": 161,
				"XcoordinateObserver": 1769.176507,
				"YcoordinateObserver": 454.526092,
				"longitudeObserver": 2.196405,
				"latitudeObserver": 48.712807,
				"XcoordinateObj": 1884.946507,
				"YcoordinateObj": 438.146092,
				"longitudeObj": 2.197981,
				"latitudeObj": 48.712671,
				"VelocityObj": 8.370000,
				"zangleObj": 1705
			},
			{
				"PerceivedObjectID": 161,
				"SumoPerceivedObjectID": "a5",
				"LastUpdateTime": 50.121000,
				"Observer": 18,
				"XcoordinateObserver": 1884.942123,
				"YcoordinateObserver": 438.143504,
				"longitudeObserver": 2.197981,
				"latitudeObserver": 48.712671,
				"XcoordinateObj": 1769.172123,
				"YcoordinateObj": 454.523504,
				"longitudeObj": 2.196405,
				"latitudeObj": 48.712807,
				"VelocityObj": 8.070000,
				"zangleObj": 3497
			},
```

```
                {
                        "PerceivedObjectID": 589,
                        "SumoPerceivedObjectID": "a19",
                        "LastUpdateTime": 50.146000,
                        "Observer": 161,
                        "XcoordinateObserver": 1769.176507,
                        "YcoordinateObserver": 454.526092,
                        "longitudeObserver": 2.196405,
                        "latitudeObserver": 48.712807,
                        "XcoordinateObj": 1931.246507,
                        "YcoordinateObj": 426.176092,
                        "longitudeObj": 2.198612,
                        "latitudeObj": 48.712568,
                        "VelocityObj": 7.300000,
                        "zangleObj": 3493
                }
        ]
}
```


7.5 Log output for UC2

Output shown by the C-ACC function, showing vehicle speed and distance between the Ego and leader vehicle. Kinematic data produced by SUMO.



7.6 Trustworthiness Claims JSON file Example


```
{
  "tchReport": {
    "trusteeReports": [
      {
        "attestationReport": [
          {
            "appraisal": 1,
            "claim": "secure-boot",
            "timestamp": "2024-07-01T14:05:15Z"
          },
```

```
          {
            "appraisal": 1,
            "claim": "control-flow-integrity",
            "timestamp": "2024-07-01T14:05:15Z"
          },
          {
            "appraisal": 1,
            "claim": "access-control",
            "timestamp": "2024-07-01T14:05:15Z"
          },
          {
            "appraisal": 1,
            "claim": "secure-communication",
            "timestamp": "2024-07-01T14:05:15Z"
          }
        ],
        "trusteeID": "Service 1"
      },
      {
        "attestationReport": [
          {
            "appraisal": 1,
            "claim": "runtime-integrity",
            "timestamp": "2024-07-01T14:05:15Z"
          },
          {
            "appraisal": 1,
            "claim": "application-isolation",
            "timestamp": "2024-07-01T14:05:15Z"
          },
          {
            "appraisal": 1,
            "claim": "secure-communication",
            "timestamp": "2024-07-01T14:05:15Z"
          },
          {
            "appraisal": 1,
            "claim": "keystore-integrity",
            "timestamp": "2024-07-01T14:05:15Z"
          },
          {
            "appraisal": 1,
            "claim": "network-intrusion-detection-report",
            "timestamp": "2024-07-01T14:05:15Z"
          }
        ],
        "trusteeID": "Infrastructure Node 1"
      }
    ]
  },
  "evidence": {
    "timestamp": "2024-07-01T14:05:15Z",
    "signatureAlgorithmType": "ECDSA-SHA256",
    "signature":
"30440220676790c8092f9830afd0141100dcf364f08a742a10ef0c4580bb761395121625022046a
3b05f282dda822c9b88b0c0732adab319074b0fc3a84137ee2f7edf21f2ba",
    "keyRef": "tch_public_key"
  }
```

7.7 Risk Assessment JSON file Example


```
{
  "content": [
    {
      "id": "663368075a7f965400954f55",
      "taraRiskassessment": {
        "id": 102,
        "name": "TARA R2"
      },
      "businessPartner": {
        "id": 1,
        "name": "Ubitech"
      },
      "attackPathProfile": {
        "id": 2,
        "name": "Information Disclosure on Camera",
        "businessPartner": {
          "id": 1,
          "name": "Ubitech"
        },
        "assets": [
          {
            "id": 502,
            "name": "Camera",
            "tags": [],
            "relationships": [
              {},
              {},
              {}
            ],
            "attributes": [],
            "taraAttributes": [
              {
                "key": {
                  "id": "CONFIDENTIALITY"
                },
                "value": {
                  "id": 1,
                  "name": "The image from the camera and location of the vehicle
can be accessed by externals"
                }
              },
              {
                "key": {
                  "id": "INTEGRITY"
                },
                "value": {
                  "id": 2,
                  "name": "The location of the vehicle can be manipulated by
externals"
                }
              },
              {
                "key": {
                  "id": "INTEGRITY"
                },
                "value": {
                  "id": 3,
                  "name": "The pictures from the camera are manipulated and it
causes collision"
                }
              }
```

```
            ],
            "tagsToString": "N/A"
          }
        ],
        "targetAsset": {
          "id": 502,
          "name": "Camera"
        },
        "targetProperty": {
          "id": "CONFIDENTIALITY",
          "description": "Confidentiality"
        },
        "elapsedTime": {
          "id": "LESS_THAN_1_WEEK",
          "description": "LESS_THAN_1_WEEK"
        },
        "expertise": {
          "id": "EXPERT",
          "description": "EXPERT"
        },
        "knowledge": {
          "id": "PUBLIC",
          "description": "PUBLIC"
        },
        "windowsOfOpportunity": {
          "id": "EASY",
          "description": "EASY"
        },
        "equipment": {
          "id": "BESPOKE",
          "description": "BESPOKE"
        },
        "attackFeasibilityRating": {
          "id": "M",
          "description": "M"
        }
      },
      "damageScenarioProfile": {
        "id": 1,
        "name": "The image from the camera and location of the vehicle can be
accessed by externals",
        "businessPartner": {
          "id": 1,
          "name": "Ubitech"
        },
        "safetyImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "financialImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "operationalImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "privacyImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "overallImpact": {
          "id": "SEVERE",
```

```
          "description": "Severe"
        }
      },
      "riskLevel": {
        "id": "H"
      }
    },
    {
      "id": "663368075a7f965400954f56",
      "taraRiskassessment": {
        "id": 102,
        "name": "TARA R2"
      },
      "businessPartner": {
        "id": 1,
        "name": "Ubitech"
      },
      "attackPathProfile": {
        "id": 5,
        "name": "Information Disclosure on GNSS",
        "businessPartner": {
          "id": 1,
          "name": "Ubitech"
        },
        "assets": [
          {
            "id": 502,
            "name": "Camera",
            "tags": [],
            "relationships": [
              {},
              {},
              {}
            ],
            "attributes": [],
            "taraAttributes": [
              {
                "key": {
                  "id": "CONFIDENTIALITY"
                },
                "value": {
                  "id": 1,
                  "name": "The image from the camera and location of the vehicle
can be accessed by externals"
                }
              },
              {
                "key": {
                  "id": "INTEGRITY"
                },
                "value": {
                  "id": 2,
                  "name": "The location of the vehicle can be manipulated by
externals"
                }
              },
              {
                "key": {
                  "id": "INTEGRITY"
                },
                "value": {
                  "id": 3,
```

```
                  "name": "The pictures from the camera are manipulated and it
causes collision"
                }
              }
            ],
            "tagsToString": "N/A"
          },
          {
            "id": 501,
            "name": "Global Navigation Satellite System (GNSS)",
            "tags": [],
            "relationships": [
              {},
              {}
            ],
            "attributes": [],
            "taraAttributes": [
              {
                "key": {
                  "id": "CONFIDENTIALITY"
                },
                "value": {
                  "id": 1,
                  "name": "The image from the camera and location of the vehicle
can be accessed by externals"
                }
              },
              {
                "key": {
                  "id": "INTEGRITY"
                },
                "value": {
                  "id": 2,
                  "name": "The location of the vehicle can be manipulated by
externals"
                }
              }
            ],
            "tagsToString": "N/A"
          }
        ],
        "targetAsset": {
          "id": 501,
          "name": "Global Navigation Satellite System (GNSS)"
        },
        "targetProperty": {
          "id": "CONFIDENTIALITY",
          "description": "Confidentiality"
        },
        "elapsedTime": {
          "id": "LESS_OR_EQUAL_THAN_3_YEARS",
          "description": "LESS_OR_EQUAL_THAN_3_YEARS"
        },
        "expertise": {
          "id": "LAYMAN",
          "description": "LAYMAN"
        },
        "knowledge": {
          "id": "PUBLIC",
          "description": "PUBLIC"
        },
        "windowsOfOpportunity": {
          "id": "MODERATE",
```

```
          "description": "MODERATE"
        },
        "equipment": {
          "id": "SPECIALIZED",
          "description": "SPECIALIZED"
        },
        "attackFeasibilityRating": {
          "id": "M",
          "description": "M"
        }
      },
      "damageScenarioProfile": {
        "id": 1,
        "name": "The image from the camera and location of the vehicle can be
accessed by externals",
        "businessPartner": {
          "id": 1,
          "name": "Ubitech"
        },
        "safetyImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "financialImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "operationalImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "privacyImpact": {
          "id": "MODERATE",
          "description": "Moderate"
        },
        "overallImpact": {
          "id": "SEVERE",
          "description": "Severe"
        }
      },
      "riskLevel": {
        "id": "H"
      }
    }
  ],
  "total": 1,
  "index": 0,
  "size": 10,
  "contentSize": 1
}
```