White Paper on Trustworthiness in Cooperative Intelligent Transport Systems (C-ITS)

CAR 2 CAR Communication Consortium

About the C2C-CC

Enhancing road safety and traffic efficiency by means of Cooperative Intelligent Transport Systems and Services (C-ITS) is the dedicated goal of the CAR 2 CAR Communication Consortium. The industrial driven, non-commercial association was founded in 2002 by vehicle manufacturers affiliated with the idea of cooperative road traffic based on Vehicle-to-Vehicle Communications (V2V) and supported by Vehicle-to-Infrastructure Communications (V2I). The Consortium members represent worldwide major vehicle manufactures, equipment suppliers and research organisations.

Over the years, the CAR 2 CAR Communication Consortium has evolved to be one of the key players in preparing the initial deployment of C-ITS in Europe and the subsequent innovation phases. CAR 2 CAR members focus on wireless V2V communication applications based on ITS-G5 and concentrate all efforts on creating standards to ensure the interoperability of cooperative systems, spanning all vehicle classes across borders and brands. As a key contributor, the CAR 2 CAR Communication Consortium and its members work in close cooperation with the European and international standardisation organisations.

Disclaimer

Document information

Number:	2320	**Version:**	1.0	**Date:**	2025-12-08
Title:	White paper on: Trustworthiness in Cooperative Intelligent Transport Systems (C-ITS)			**Document Type:**	WP
Part of release	N.a.				
Release Status:	Public				
Status:	Final				

Table 1: Document information

Changes since last release

Date	Changes	Edited by	Approved
2025-12-08	Initial release	Release Management	Steering Committee

Table 2: Changes since last release

Table of contents

List of tables

1 Executive Summary

Cooperative Intelligent Transport Systems (C-ITS) promise to revolutionize road safety, traffic efficiency, and driver convenience. As these systems become increasingly interconnected and autonomous, trustworthiness emerges as a foundational requirement to ensure stakeholder confidence and user acceptance.

Trustworthiness, as defined in ISO 5723, refers to the ability to meet stakeholders' expectations in a verifiable way. This definition is generic and applies across systems. However, its application in C-ITS introduces specific challenges due to the dynamic, distributed, and safety-critical nature of vehicular networks.

This white paper elaborates on the specific meaning of trustworthiness in the context of C-ITS according to C2C-CC specifications, explaining not only what the term implies in a general sense but what it must deliver in this domain. In particular, for C-ITS to be deemed trustworthy, it must:

- Ensure verifiable system behaviour that is consistent, safe, and reliable under variable conditions
- Protect user privacy while providing mechanisms for accountability and oversight
- Guarantee authenticity and integrity of messages through a secure, transparent PKI infrastructure
- Support availability and robustness in communication and system functions
- Adapt to threats and disruptions with resilience and crypto-agility
- Enable independent certification and compliance validation beyond self-declaration

By detailing these expectations and evaluating the gaps between current capabilities and required outcomes, this document guides stakeholders toward designing and maintaining trustworthy C-ITS ecosystems.

2 Introduction

C-ITS enables communication between vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and networks (V2N), forming a complex ecosystem that relies heavily on real-time data exchange, distributed computing, wireless networking, and cryptographic frameworks.

In general terms, trustworthiness means that a system behaves as expected and can be verified to do so. However, the application of this concept to C-ITS is more nuanced and demanding. In C-ITS, trust must be established not only in static systems but across highly dynamic, decentralized actors with no prior relationship or guaranteed connectivity.

Therefore, the trustworthiness of C-ITS must be engineered explicitly: systems must be demonstrably safe, secure, and privacy-preserving. This involves technical assurance (e.g., cryptographic protections), organizational trust (e.g., governance structures), and continuous validation (e.g., certification schemes).

This paper builds upon the terminology and concepts outlined by the Car-to-Car Communication Consortium (C2C-CC), extending them into a strategic framework for understanding and achieving trustworthiness in the evolving C-ITS landscape.

3 Dimensions of Trustworthiness in C-ITS

The ISO 5723 standard defines trustworthiness as "the ability to meet stakeholders' expectations in a verifiable way." Within the C-ITS domain, trustworthiness spans multiple dimensions. Each contributes to the overall dependability, acceptance, and societal legitimacy of C-ITS technologies. Below we analyse each of these dimensions, outlining their definitions, implications for C-ITS, and current challenges.

3.1 Accountability

Being answerable for actions and decisions, particularly in the case of accidents or system failures affects both the operators of C-ITS stations, Certification Authorities (CAs) as well as vehicle automation providers and/or vehicle drivers. Legal and regulatory frameworks for accountability are still under discussion and accountability needs may conflict with privacy requirements. There is a growing need for transparent audit trails that balance user anonymity with the need for forensic evidence.

3.2 Accuracy

Accuracy is necessary to ensure that information obtained from observation and measurements is close enough to the true physical values on the road, to fulfil application requirements. In C-ITS, since the equipment and related vehicle sensors are mounted in stock-vehicles owned by private customers and operated under harsh conditions, it is difficult to guarantee the optimal accuracy. Therefore, information about the closeness of a measurement is provided in the C-ITS messages through confidence related information.

3.3 Authenticity

Authenticity in C-ITS ensures that entities—vehicles, infrastructure, or users—are who they claim to be in terms of technical capabilities, i.e., the functionalities they implement and the compliance with standards and interoperability specification. In C-ITS, authenticity is achieved via digital certificates and signatures governed by Public Key Infrastructure (PKI) such as the EU CCMS. The current self-declaration model for EU CCMS compliance poses risks for false claims that jeopardize the authenticity, highlighting the need for independent certification of C-ITS stations.

3.4 Availability

Systems and services must be reliably accessible when needed. In C-ITS, availability of the overall system is achieved by the ad-hoc broadcast model and redundancy through message repetition. However, future systems must also address load balancing, channel congestion, and fault tolerance. Availability aspects of single C-ITS stations are not dealt with since they are technically and economically not very viable.

3.5 Controllability

The system must remain under human or authorized control, especially in emergency or degraded situations. In C-ITS, control is usually maintained by the vehicle operator or system administrator, though autonomous decision-making challenges this model.

3.6 Information Security

Information security is mainly covered by integrity and authenticity. Confidentiality is only used on limited interfaces.

3.7 Integrity (Data and System)

Integrity ensures that data has not been altered maliciously or by accident. In C-ITS, message signing supports data integrity, while system-level integrity relies on conformance to standards. The current gap lies in the enforcement of the EU CCMS compliance and independent verification of C-ITS station.

3.8 Privacy

C-ITS must protect users from identification, surveillance, and misuse of data. Confidentiality of unicast communications, pseudonymization techniques for broadcast communication, incl. short-lived certificates, and decentralized data handling are standard practices, though emerging use cases may challenge these protections.

3.9 Quality (Data and System)

Data quality (accuracy, timeliness) and system quality (service delivery) are essential in C-ITS. As use cases evolve – such as in cooperative perception or collective awareness – so too must quality metrics and validation mechanisms. C-ITS Release 2 introduces higher quality demands on both transmitters and receivers. Data quality requirements go mostly hand-in-hand with accuracy requirements.

3.10 Reliability (Cybersecurity and System)

Reliable systems behave consistently and meet expectations over time. While C-ITS Release 1 did not include formal reliability metrics, Release 2 introduces operational requirements, particularly for centralized components like the CPOC.

3.11 Resilience (Governance and System)

Resilience refers to the ability to recover from or adapt to disruptions even with a less performant or degraded mode. In C-ITS, this includes cryptographic agility, redundant systems, and robust incident response processes. Future systems must anticipate environmental threats, software bugs, and supply chain vulnerabilities.

3.12 Robustness

Systems must perform under a wide range of conditions. C-ITS systems are inherently distributed and decentralized, supporting robustness. Further improvements include support for multiple GNSS constellations and hardened components for vehicular environments.

3.13 Safety

A C-ITS system must not endanger users or the public due to accidental harm or failure. For example, interruption of service or incorrect data can pose significant safety risks. C-ITS must therefore account for both Functional Safety (FuSa), i.e. the absence of unacceptable risk to persons due to hazards caused by malfunctioning behaviour of electrical or electronic systems and Safety of the Intended Functionality (SOTIF), i.e. the absence of unreasonable risk resulting from functional insufficiencies or misuse.

3.14 Security

Security encompasses protection of systems from intentional attacks. Due to the overlap with safety (see 2.3) and information security (see 2.6), here security is intended as cybersecurity, i.e. the safeguarding of C-ITS stations and the EU CCMS from cyber risks. In fact, broader system-level threats, such as denial of service or spoofing, require continued vigilance and adaptive countermeasures for the station operators.

3.15 Transparency (Information and System)

C-ITS System design and data handling must be open and understandable. Transparency builds trust among users and stakeholders and facilitates debugging, auditing, and regulatory compliance.

3.16 Usability

C-ITS must be effective, efficient, and satisfying to use. Human-machine interface (HMI) design, system feedback, and seamless integration are key to ensuring high usability levels.

4 Current Gaps and Future Directions

Although Release 1 of C-ITS introduced foundational mechanisms for trustworthiness, gaps remain in assurance, standard enforcement, and real-world testing. These gaps must be addressed to create a secure and reliable transportation system. The following table shows the differences in support for trust between the available C2C-CC Release 1 and the planned Release 2. The text differentiates between (vehicle) C-ITS stations and the overall system-of-systems composed of those stations.

Dimension	Release 1	Release 2
Accountability	For manufacturers: based on self-declaration of compliance for C-ITS Stations	For manufacturers: Formal (product) accountability is envisioned through compliance testing. For vehicle automation and/or drivers, accountability aspects are still to be studied in detail vs. privacy and functional safety.
Accuracy	Accuracy information is provided through confidence levels for selected information objects in C-ITS messages	Same as Release 1
Authenticity	According to C-ITS Security Policy and based on EU CCMS (ECTL L1 and L2)	According to C-ITS Security Policy and based on EU CCMS (ECTL L2 and higher levels)
Availability	Overall System: ensured through the redundancy of the distributed system and the broadcast nature of C-ITS	Additionally, requirements on the availability of the single C-ITS stations may be defined
Controllability	Based on single system operator principle	No change w.r.t. Release 1
Information Security	See Authenticity and Integrity	See Authenticity and Integrity
Integrity (data)	According to C-ITS Security Policy and based on EU CCMS (ECTL L1 and L2)	According to C-ITS Security Policy and based on EU CCMS (ECTL L2 and higher levels)
Integrity (system)	Based on C-ITS station compliance with standards and profiles	Additionally, system integrity checks may be added.
Privacy	Based on EU CCMS and on storage rules for personal data	Same as Release 1
Quality (data)	Selected data quality requirements (e.g., on PoTi)	Higher requirements
Quality (system)	Selected dissemination requirements	SOTIF approach for systems and their services
Reliability (cybersecurity)	According to C-ITS Certificate Policy and based on EU CCMS (ECTL L1 and L2)	According to C-ITS Certificate Policy and based on EU CCMS (ECTL L2 and higher levels)
Reliability (system)	Overall System: ensured through the inherent	In release 2 the focus will be on reliable use of the communication channel(s)

	redundancy of the distributed system	
Resilience (governance)	There is a process to collect field-operations feedback and to respond to service issues and disruptions.	It is envisioned to address crypto resilience in future EU CCMS updates.
Resilience (system)	Systems are remotely managed to detect and respond to issues and maintain their function.	In release 2 the focus will be crypto resilience and communication medium redundancy
Robustness	Overall System: Based on distributed system design	Additionally in Release 2, the system should be GNSS multi-constellation capable
Safety	n.a.	Shall be based on FuSa and STIF
Security	Only Information Security aspects are covered	Only Information Security aspects are covered
Transparancy (information and system)	Covered by nature of C-ITS since it is based on information sharing	Covered by nature of C-ITS since it is based on information sharing
Usability	Covered by nature of C-ITS since it is end-user oriented	Covered by nature of C-ITS since it is end-user oriented

Table 3: differences in support for trust between the available C2C-CC Release 1 and the planned Release 2

The following table summarizes some of the most critical gaps and potential improvements.

Aspect	Current Gap	Future Direction
Compliance	Self-declaration without oversight	Independent third-party certification
Data Quality	Assumed accuracy, no assessment scheme	Standardized data quality metadata and audits
Reliability	No formal service-level metrics	Definition of SLAs and performance benchmarks
Resilience	Lack of crypto agility	Post-quantum cryptography and redundant networks
Privacy vs Accountability	Hard to reconcile traceability with anonymity	Privacy-preserving accountability protocols

Table 4: Potential improvements

5 Conclusion

Trustworthiness in C-ITS is a prerequisite for public confidence and successful deployment. The dimensions described herein must be treated not in isolation but as an interrelated system that governs the lifecycle of C-ITS services.

As C-ITS matures, industry stakeholders must collaborate to strengthen certification models, evolve cryptographic frameworks, and refine performance expectations. Future releases must consider not just technical compliance but also ethical, legal, and societal acceptance of connected transport technologies.

Trust cannot be retrofitted – it must be designed, measured, and maintained from the beginning.

6 References

[1] ISO 5723: Vocabulary for Trustworthiness
[2] ETSI EN 302 665: C-ITS Communication Architecture
[3] ISO/PAS 21448: Safety of the Intended Functionality (SOTIF)
[4] ISO 26262: Functional Safety