Trusted Integrity and Authenticity for Road Applications (TIARA)

Final Report

Deliverable D1.2

Date 30/09/2025

Author(s) Alan Walker, Pete Lockhart

CEDR Call 2022 Data: Integrity, Authenticity, and Non-Repudiation integrated in Trust Models for C-ITS applications

1 Introduction

1.1 Project Facts

Duration:	22/11/2023 – 30/09/2025
Budget:	EUR 264 985.75
Coordinator(s):	Alan Walker, Pete Lockhart, c/o AESIN, UK e-mail: alan.walker@syselek.com, tel: +44 7960 495253
Partners:	AESIN/Techworkshub, UK
	Sintef, Norway
	Traficon, Finland
	TML, Belgium
PEB contact(s):	Maxwell Ash, National Highways, UK
	Peter Lewyllie, Vlaanderen, Belgium

1.2 About TIARA

1.2.1 Background

The objective of the *Trusted Integrity and Authenticity for Road Applications (TIARA)* project was to provide National Road Authorities (NRAs) with an improved understanding of what is required to achieve a trustworthy and secure connected vehicle data infrastructure. The availability of data has allowed road users and NRAs to benefit from new business models. To deliver these benefits, the connected vehicle data infrastructure must be trustworthy and trusted, i.e., secure, with assurances that it is managed to achieve privacy for all stakeholders.

As more Cooperative Intelligent Transport Systems (C-ITS) services develop in Europe, and road users access and share more C-ITS data through open border countries, NRAs will need to ensure greater interoperability through common approaches to connected systems. Data trust is therefore paramount.

CEDR undertook three projects to research how NRAs can maintain and share the digital road infrastructure data and improve the use of third-party data by NRAs. The TIARA project was delivered in close liaison with CEDR and its members, as well as the two further research projects funded in the CEDR 2022 Research call on Data, Topics A (DROIDS, 2023) and B (PRESORT, 2023), introduced in Figure 1.

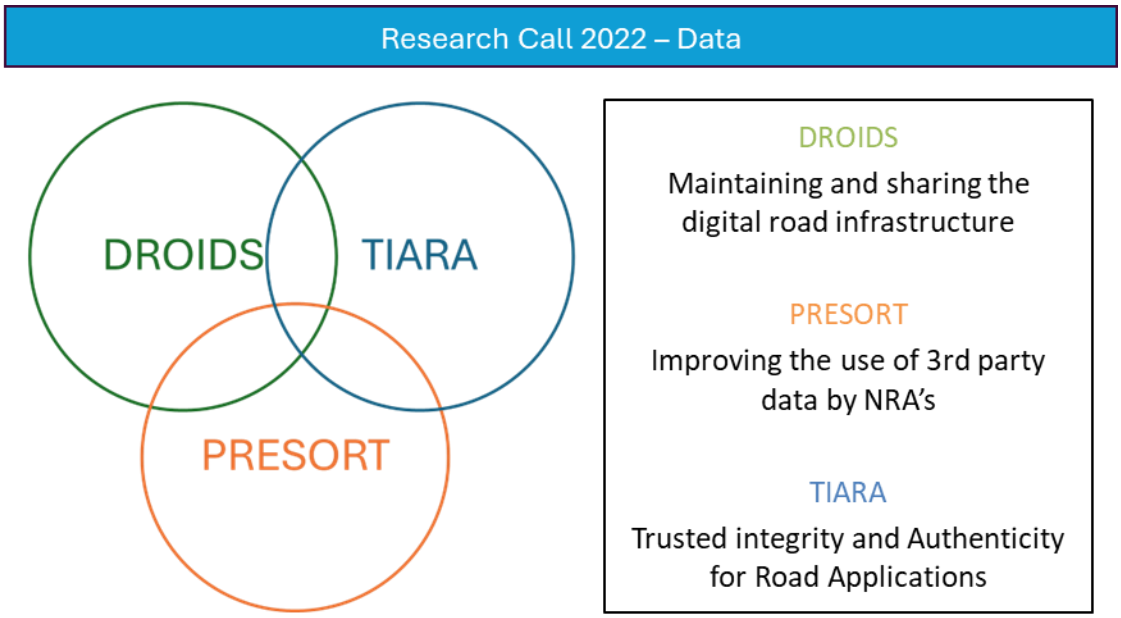

Figure 1: Three projects in the CEDR 2022 Research call on Data.

Since the C-Roads Platform has started (C-Roads, 2024), several Intelligent Transport Systems (ITS) programmes have been rolled out and it has been identified that there are key elements that the NRAs will need to understand before implementing these systems more widely. The TIARA project was designed to address the two key areas of Trust and Privacy

in C-ITS applications. The first subject, Trust, concerns an understanding of the implementation of trust models that could protect C-ITS data. The second subject, Privacy, concerns an understanding of the impact of processing user personal data, including location.

Three broad research areas were identified:

- Trust for C-ITS applications, to develop practical guidance for the implementation of Public Key Infrastructure (PKI) for C-Roads,
- Legal and ethical ramifications for NRAs when making use of C-ITS data, and of how these change the role of the NRAs,
- Privacy impact of the processed road user location data, and recommendations to improve the location privacy-preservation for NRAs.

An experienced team of European research organisation gathered under the coordination of AESIN/Techworkshub, the UK-based member trade association, to address this complex topic through network engagement with organisations and individuals possessing experience and technical expertise, yet independent of any specific solution vendors.

AESIN/Techworkshub belongs to the Techworkshub organisation, through which it has access to member experts in both transport and Internet-of-Things (IoT) security sectors.

SINTEF, as an independent and non-profit research organisation, has independent technical expertise and deep experience from PKI deployments in multiple sectors.

Traficon has longstanding experience of independent work with NRAs, specifically legal and ethical expertise of particular relevance to this project.

TML, bridging the gap between university and private sector, is an independent open and transparent organisation with extensive experience of data analyses and privacy ramifications.

1.2.2European Cooperative Intelligent Transport Systems (C-ITS) and Services

C-ITS is a subset of standards for ITS. C-ITS services exchange trusted and secured data between vehicles, roadside infrastructure, control and services centres in the cloud, and other road users. The European framework for trusted and secure C-ITS communication, using PKI, is the European Union C-ITS Credential Management System (EU CCMS) (C-Roads, 2024).

ITS use information and communications technology in transport including infrastructure, vehicles and users, as well as traffic and mobility management. Interfaces with other modes of transport are also included. ITS aims to improve transport safety, reliability, efficiency and quality (C-Roads, 2024).

C-ITS services are ITS services that are provided using V2X communications as agreed in C-ITS specifications. The C-Roads Platform defines C-ITS service or “application” as “a clustering of use cases based on a common denominator, for example, an objective such as awareness or a context like road works” (C-Roads, 2024). C-ITS services in Europe have been proposed under EU strategies and studies, such as European Commission (EC) COM(2016) 766 and C-ITS Platform (2016) (CCAM, 2021). The services, and their timeframe for likely implementation, are indicated in Figure 2.

The C-Roads Platform has also defined European C-ITS specifications. These comply to C-ITS standards. The CAR 2 CAR Communication Consortium (C2C-CC) has developed the Basic System Profile, which has been harmonised in the C-Roads specification for road infrastructure. C2C-CC members include European and international vehicle manufacturers, equipment suppliers, engineering companies, road operators and research institutions (C2C-CC, 2002).

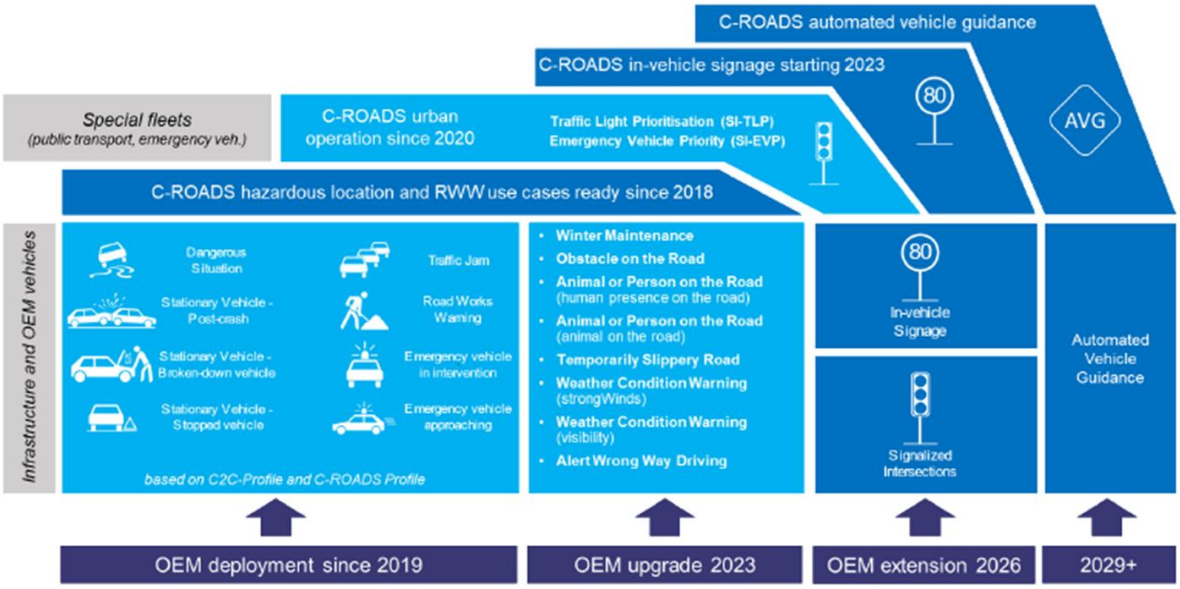

Figure 2: The C-Roads Platform for harmonisation of C-ITS deployment.

1.2.3European C-ITS Pilots and Issues

Since C-Roads started, several European trials of C-ITS have been ongoing. However, there are elements that road authorities will need to understand before implementing C-ITS systems more widely:

- Roll-out of PKI systems

The PKI systems required for C-Roads and C-ITS systems are comparatively complex. Certificates are generated and loaded into a vehicle, and are regularly rotated for security and privacy reasons, meaning that there is a large throughput of certificates. The PKI needs to support this generation of certificates and needs to support the regular verification of messages. Road authorities need support and guidance to better understand how to implement the PKI systems required.

- How NRA's ethical and legal obligations change with connected road infrastructure

C-ITS systems represent an evolution of the role of the road authority, from building and maintaining roads, through traffic management technology, to directly transmitting data to the road user. This is a change in the responsibility of the NRA. The NRA needs to ensure that the data they provide maintains integrity, that the road user understands the data they are receiving, and how the collected data is being used. As such, NRAs must understand their ethical responsibilities to customers and other users of the data that they collect.

- Privacy of road operators' customers' data

To ensure road users trust the lawful and sensible use of their data by road operators, road authorities must be open and transparent about the data that is collected and for what it is used or could be used. Opinion 3/2017 of Art. 29 Data Protection Working Party indicates that identifying the physical location of a road user can be sufficient to trace back to an individual in a population (taking account of regular travel patterns within certain precision). Several European road operators process location data from road users to optimise signalised intersections (e.g., Flanders and the Netherlands) or to warn about slow moving vehicles. Measures must be implemented to make such re-identification more difficult, and road authorities should understand to what extent these measures are sufficient to make reidentification "reasonably" impossible.

1.2.4TIARA Project Scope

The scope of the study and key concepts were defined in collaboration with CEDR and the TIARA project partners, and were limited primarily to C-ITS. Stakeholders from independent organisations and individuals with key expertise also provided input for the project scope through workshops. The linkages to other CEDR research project scopes are indicated in Figure 3.

Secondary technologies also include ITS. Although ITS have different standards and specifications than C-ITS, it was seen beneficial to have broader views and experiences on data accuracy, quality, and accountability, and the consequences of inaccuracy.

While C-ITS services have been implemented in recent years at the European roads, there is significantly more experience on traditional ITS services and data accuracy. Furthermore, many ITS services have similarities with the initial C-ITS services, e.g., so called “Day 1 services”, with differences around the communication medium, standards, specifications and communication protocols. For example, road operators may already share slippery road warnings to road users using ITS or C-ITS.

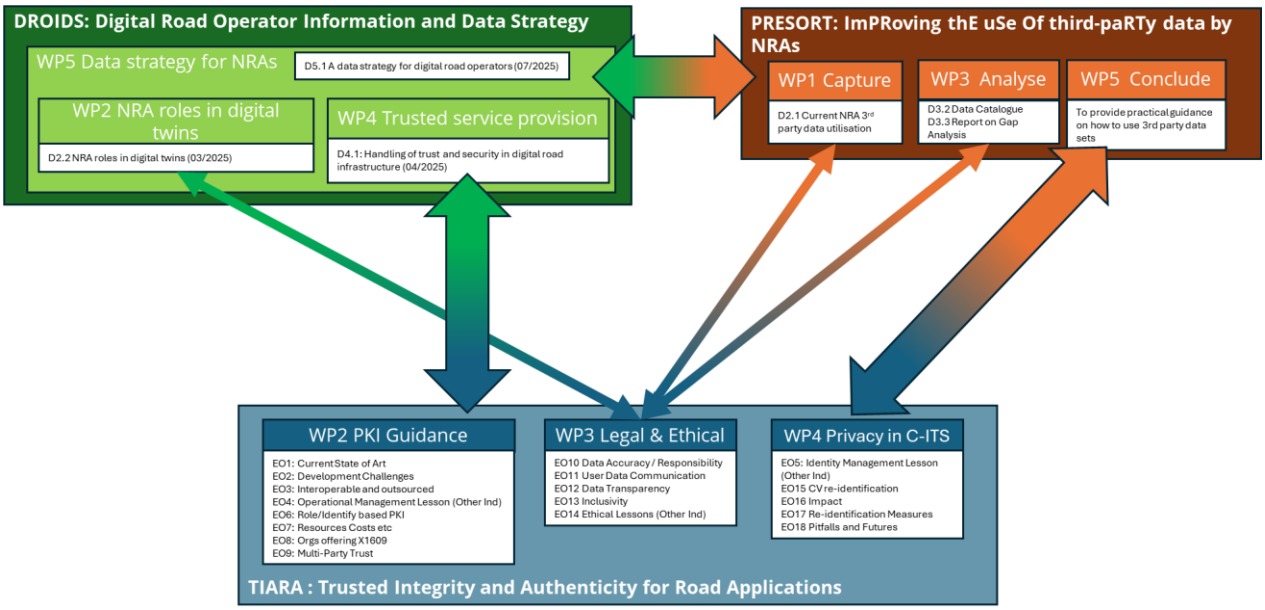

Figure 3: Linkages between scopes of the three CEDR research projects.

1.3 Expected Outcomes

The following Table 1 lists the different Expected Outcomes (EOs) addressed within the three technical study topics of the project.

Table 1: Expected Outcomes and associated workpackages.

Expected Outcome		Workpackage(s)
EO1	Review of the current state of PKI roll-out in European NRAs (state of the art)	**WP2** Trust for C-ITS applications to develop practical guidance for the implementation of PKI for C-Roads
EO2	Analysis of the issues and problems that NRAs will encounter when developing PKI.	
EO3	Advice for building the organisations required to run a nationwide PKI that is interoperable with Europe, and advice on outsourcing PKI services.	
EO4	Lessons from other industries (finance, healthcare, etc.) on operation of a PKI.	
EO6	Guidance on the use of role-based and identity-based PKI.	
EO7	Analysis resources required to run C-Roads PKI, including how the cost and computational requirements scale, and the administration required for certificate and key management.	
EO8	View of commercial and public organisations offering X.509 and 1609.2 PKI functionality.	
EO9	Advice for developing PKI systems that provide trust across multiple parties, for example extending the trust infrastructure to road workers or maintenance companies.	
EO10	Guidance on the responsibility of the road authority to ensure that data is accurate, and the accountability when inaccurate data is sent.	**WP3** A review of the legal and ethical ramifications for NRAs when making use of C-ITS data, and of how these change the role of the NRA.
EO11	Guidance on best practice for the communication of data and its limitations with road users.	
EO12	Views on how to be open and transparent with roads users on the use of data.	
EO13	Review of how communications around the use of C-ITS systems and data can be ensured to be inclusive of road users across technical ability. Guidance on developing C-ITS services that are inclusive of road users across technical abilities.	
EO14	Lessons from other industries on the ethical use of data.	

cont.

Expected Outcome		Workpackage(s)
EO5	Lessons from other industries (license plate registry, etc.) on governing of identities.	**WP4** Privacy in C-ITS applications
EO15	Overview of research into Connected Vehicle re-identification or deanonymisation and research into associated preventive measures.	
EO16	Analysis of the information about road users that could be leaked from C-ITS data and the potential impact on the data subject.	
EO17	Analysis of the current measures and recommendations for additional measures to make re-identification reasonably impossible.	
EO18	Analysis of pitfalls that would increase the risk of re-identification: what to avoid in future use cases? What data cannot be added?	
EO19	Recommendations for how the understanding of the privacy provided by the system can be maintained as new use cases and as the use of data becomes more widespread.	

1.4 Purpose of this report

This Final report provides an overview of the TIARA project activities and outcomes, accompanying the Final technical reports from the three technical studies individually addressed by WPs2-4.

1.5 Acronyms

C2C-CC	Car 2 Car Communication Consortium
CA	Certificate Authority
CEDR	Conference of European Directors of Roads
C-ITS	Cooperative Intelligent Transport Systems
C-Roads	European initiative to test and implement interoperable C-ITS services.
C-V2X	Vehicle-to-everything communication using both cellular and local/direct connection
DROIDS	Digital Road Operator Information and Data Strategy
EC	European Commission
EO	Expected Outcome
EU CCMS	EU C-ITS Credential Management System
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
ICT	Information and Communications Technology
IoT	Internet-of-Things
ITS	Intelligent Transport Systems
ITS-G5	Short-range vehicle communication standard based on IEEE 802.11p at 5.9 GHz
KOM	Kick-off Meeting
NAP	National Access Point
NRA	National Road Authority
PEB	Programme Executive Board
PKI	Public Key Infrastructure
PRESORT	Improving the Use of Third-Party Data by NRAs
TIARA	Trusted Integrity and Authenticity for Road Applications
TRA	Transport Research Arena
V2X	Vehicle-to-Everything
WP	Work package

2 Outcomes

2.1 WP1 Project management

Project meetings

Project meetings took place with partners bi-weekly and with PEB project representatives monthly (i.e. every second meeting). These meetings tracked project progress against plan.

Project PEB meetings and workshops

A project KOM to review and confirm the project plan was held on 22/11/2023 involving all partners and PEB members, and a commencement workshop to review and elaborate the research questions, and to ensure that all prior work was identified and available before undertaking the project work, was held on 20/12/2023 involving all partners and PEB members.

TIARA project progress was presented to the PEB at online meetings on 03/10/2024 and on 16/06/2025, and progress was also presented to the PEB at face-to-face meetings in Ghent on 17/06/2024 and in Utrecht on 23/01/2025. Workshops were also conducted at the face-to-face meetings.

TIARA project partners also supported online workshops organised by DROIDS and PRESORT projects.

Project reports

An Inception Report based on the outcomes from the KOM and commencement workshop was delivered to the PEB on 15/02/2024.

An Interim Project Report (D1.1) summarising project progress was delivered to the PEB on 02/09/2024. Three Interim Technical Reports (D2.1, D6.1, and D8.1) detailing the technical findings were also delivered to the PEB on 02/09/2024.

Three Final Technical Reports (D2.1/D2.2 “Operation of Public Key Infrastructures: State-of-the-art and best practices, and Guidance on the implementation of C-ITS PKI”, D6.2 “NRA Guidance on Legal and Ethical Use of Data”, and D8.2 “Connected Vehicle De-anonymisation Research Review and Impact Study”) were delivered to the PEB on 04/07/2025.

This Final report includes summaries from these Final Technical Reports.

2.2 WP2 PKI Guidance Development

Background

Digital certification is a cornerstone of trust, security, and interoperability in C-ITS. PKIs enable secure authentication and data exchange between C-ITS stations, such as vehicles, roadside units, and traffic management systems. A PKI ensures the trustworthiness of digital certificates through a defined framework of roles, policies, procedures, and secure infrastructure.

State of PKI roll-out in Europe (EO1)

Operational deployments of C-ITS PKIs remain limited in Europe. Countries such as Austria, Germany and France have made notable progress to establish a significant C-ITS PKI and credential management nationally and locally. Compared with a European roll-out, the national system offers more control but is probably less cost-effective. Other countries, such as Denmark participating in the C-Roads platform, Norway with some mobile infrastructure, Italy, The Netherlands, and UK, are pursuing limited demonstrations and pilots, although these focus more on functionality than security. Cross-border C-ITS services, such as related to safety, customs, or payments, are yet to be addressed or harmonised.

Some NRAs are using existing PKI solutions from other operators, with the goal to be part of the harmonised, interoperable EU CCMS using the EU Root Certificate Authority (CA), with enrolment and authorisation currently operated by Eviden from France. More than 40 actors are currently connected to the EU Root CA.

NRA issues when developing PKI (EO2)

To support a harmonised approach, the EC has introduced the EU CCMS, which defines a common trust hierarchy for CAs. Coordinated action of multiple parties, including OEMs, to adopt the EU Root CA and get their C-ITS services "approved", will be needed to succeed. Without managed transitions between different PKIs, seamless interoperable communication will not be achieved across borders and across different systems and brands. Maintaining compliance of hardware while regulations and protection profiles evolve over years, yet legacy vehicles persist on the roads, adds cost and complexity. Operating costs dominate considerations.

Organisational and outsourcing considerations (EO3)

NRAs are expected to serve as key trust anchors within the European trust model. Strict processes and significant expertise are required but these can be challenging to maintain consistently over time. Finding the required niche expert skills is difficult. Due to the high complexity and resource demands of PKI operations, most states think that the technical implementation of their PKI solution will be outsourced to specialised service providers responsible for implementation and operation, but that the state or NRA will be the solution owner.

PKI operational lessons from other sectors (EO4)

Operational practices should reflect organisational structures. Avoiding hierarchical structures makes PKI more useful in real-world use cases. Too much focus on technology, and not enough on organisational aspects, particularly skills and resources to operate a PKI, can lead to an expensive and unsuitable PKI design.

Purpose designed PKIs are more useful than one-size-fits-all. The EU CCMS appears to be a good foundation for the European C-ITS architecture, provided that the various stakeholders are assigned appropriate roles and responsibilities. The choice of trust model when dealing with inter-organisational PKIs is common to other sectors. C-ITS needs to move from "shell-based" protection to transaction-based protection, although over-engineering is likely before the adoption of standards is widespread. Using short-lived pseudonym certificates instead of traditional revocation mechanisms can minimise complexity and avoid potential response time issues when checking certificate validity. Understanding number of users and easily changing user credentials will be helpful.

Other issues include too weak keys, unnecessarily long certificate lifespans, improper protection of private keys, and lack of policy consistency. Information technology, healthcare, finance, e-government, telecoms, education, maritime and aviation sectors highlighted fundamental PKI management challenges:

- Lack of skills and resources to operate a PKI.
- Lack of investments in modern PKI infrastructures, leaving outdated manual PKI management methods.
- Attackers will exploit weak credentials, too weak keys, unnecessarily long certificate lifespans, improper protection of private keys, lack of policy consistency.
- Poor key management practices and compromised/rogue CAs should fail PKI management and cryptography audits.
- Data theft, service disruption, and malware distribution are high risk.

Role-based and identity-based PKI (EO6)

Local private PKI is needed if a subset of roles is required, with different types of users, such as police vehicles, ambulances, maintenance vehicles, repair shops, etc. Different certificate roles may be required – e.g., permissions for local transit buses within one city, rather than for all transit buses nationally. C-Roads and C2C-CC are working to harmonise the more common use cases. The certificate validity management (revocation or short-lived) will also depend on the type of application/service and type of users.

Resources to run C-Roads PKI (EO7)

Although there are several private companies providing PKI services, it is important to ensure that C-ITS specific needs are properly identified and met. A recurring challenge is the scarcity of PKI specialists in the transport sector. As a result, many NRAs and infrastructure operators are expected to rely on outsourced PKI services. This shift necessitates robust outsourcing models, clear contractual frameworks, and close oversight to ensure compliance, reliability, and scalability. Ultimately, the success of C-ITS deployment in Europe will depend on strong cross-sector collaboration, alignment between technical and policy layers, and the ability to manage complexity while delivering secure, interoperable, and user-centric services. NRAs require this guidance when establishing and applying best practices.

Commercial and public organisations offering X.509 and 1609.2 PKI functionality (EO8)

Competition between short-range communication (ITS-G5), adopted by VAG, and long-range communication (C-V2X), adopted by other vehicle manufacturers, may lead to a hybrid solution, where both standards will be used, potentially with parallel PKI systems for different services according to the required speed of communication (1609.2 certification for ITS-G5 and X.509 certification for C-V2X).

Even though C-ITS is at an "early stage", there are already some providers that offer C-ITS PKI services, albeit prices are expensive and a hybrid short-/long-range solution may cost even more. For the most part, these providers have information security as (part of) their core business, but there are also a few actors from the automotive industry, such as VAG, who have decided to establish and operate their own PKI. Operating a PKI requires specific competence and resources. NRAs can therefore implement PKI by undertaking all activities themselves, or procure parts of the system, or procure the entire system as a package.

Extending the trust infrastructure across multiple parties (EO9)

Identifying how C-ITS applications will be monetised, i.e., who will benefit and who will pay, is probably the most challenging part. More data sharing between vehicle manufacturers and NRAs will be required for effective provision of high-quality relevant information according to the desired services. Other third parties should be engaged, such as maintenance companies to provide use cases involving road workers.

Guidance and recommendations for NRAs for the future

1. Combine specialist skills and trusted outsourced service providers to build expertise.
2. Follow CCMS and ensure cross-border interoperability to align with EU trust model.
3. Coordinate across NRAs, OEMs, telecoms, and cities to foster collaboration.
4. Avoid vendor lock-in, promote open interoperable standards, support hybrid comms.
5. Ensure robust security by continuous monitoring, readiness, and independent audits.
6. Plan for flexibility and scalability, with modularity, and backwards compatibility.
7. Share costs and responsibilities (with use of e.g. Public-Private Partnerships, automation, and long-term contracts).
8. Focus on user trust and adoption by delivering reliable, high-quality services.

NRAs should also focus on:

- Authenticating and controlling users,
- Managing the expiration of certificates,
- Reducing PKI infrastructure complexity, and
- Standardised use cases and message formats.

2.3 WP3 Legal and Ethical Aspects

Data accuracy and accountability (EO10)

There are no direct technical requirements outside of required data formats (e.g., DATEX II) related to ITS or C-ITS data accuracy nor quality in European legislation. However, Member States are required by the EU Real-time traffic information (RTTI) delegated act 2022/670 legislation to set up National Access Points (NAPs), make the data available, communicate inaccuracies, provide data quality parameters, and follow minimum quality requirements agreed with relevant stakeholders. These are further implemented in Member States, depending on legislation and policies, by the road operator or NRA. Other ITS and C-ITS relevant European legislation include the EU Product Liability Directive (EU, 2024), which includes software and related services, where navigation systems providing traffic data are mentioned as an example of a product with safety liabilities.

Communicating data limitations to road users (EO11)

It is important to know who the users are and what are their needs, so users need to be consulted throughout the data and service development life cycle to ensure inclusivity.

the NAP and the national or regional interchange nodes or clouds are the main channels for data publication. Road operators should also inform data users about the quality of the data. The first user group contained different road user stakeholders referred to in the ITS Deployment directive (EU, 2010), such as vehicle owners or vulnerable road users. The second user group had specific needs, such as mobility impairment or disabilities.

Transparent data use (EO12) and Ensuring inclusive C-ITS systems and data (EO13)

The following recommendations for transparent and inclusive communication were mainly based on UK Government guidance (Data Quality Hub, 2021) and workshop results:

- Follow legislation, rights and principles
- Explain importance of data quality communication
- Develop effective, bidirectional communication with users and stakeholders
- Make communication user-centric
- Make communication accessible and inclusive
- Practice transparent and reliable data quality and service communication
- Ensure privacy and data protection in communication
- Communicate in a timely and responsive manner
- Engage with data providers and users
- Provide education to users
- Provide communication guidelines for all communication
- Create a process for continuous communication monitoring and development
- Practice proactive risk management in communication

Road users' technical abilities (EO13)

- Human Machine Interface (HMI) development needs to reflect road users' technical abilities. Inclusive, universal, and usable principles make systems easy to use.
- No legislation or regulation directly relates to service development or HMIs. The ITS Deployment directive (EU, 2010) does contain indirect references for safe service deployment. Although in-vehicle systems have developed considerably since 2008, the EC's recommendations for safe and efficient in-vehicle information and communication systems (EU, 2008) are still valid and can be applied.
- Road operator responsibilities extend to their agreements and contracts with road maintenance contractors. For example, if a contractor is required to use a service or third-party application, the road operator needs to ensure the service usability.
- The barriers and opportunities identified included missing inclusive regulation, enhanced co-creation, and simplifying GDPR compliance messaging. Co-creation requires collaboration between road operators, private industry, and road users, to meet user needs. There is a lack of inclusivity or HMI regulation, but with sufficient collaboration this should not be needed.
- Inclusive services require extensive modelling, simulation, testing, and piloting with the road users. If road operators decide to develop their own services, they need to carefully consider if those services are core business priorities. Multisided business models could lead to high development and maintenance costs so discrepancies between potential services and road operators' responsibilities should be evaluated.

Ethical data use (EO14)

The UK Government's data ethics framework (Data Ethics Framework, 2020) is recommended for road operators and contractors. The principles of transparency, accountability, and fairness guide road operators along with practical actions, which should be documented and shared with the community. It is ethical to provide data quality information with data and implement an organisational code of ethics.

Potential road users' data leakage and impact (EO16)

- Data and services delivered by NRAs or subcontractors are the NRAs' responsibility.
- Inclusive communication requires engagement with a wide range of user groups.
- Potential leakage risks and their potential impact need to be communicated to road users along with mitigation actions. NRAs need data ethics policies and processes.

Guidance and recommendations for NRAs the future

1. Embed legal, contractual, and ethical responsibilities for data accuracy in operations.
2. Identify road users, communicate and involve in real-world service development.
3. Acquire expertise on C-ITS services, use cases, and their limitations.
4. Establish inclusive and transparent communication.
5. Develop inclusive services using human-centred design principles.
6. Apply ethical principles and processes for data use.
7. Carry out risk evaluation when communicating and developing ITS/C-ITS services.

2.4 WP4 Privacy in C-ITS Applications

Reidentification or deanonymisation and preventive measures (EO15)

Privacy risks associated with C-ITS messages can reveal sensitive information about vehicle locations and user behaviours, even when anonymisation techniques are applied. There are suppression and generalisation strategies that enhance privacy protections to counter re-identification or deanonymisation threats. Technical preventive measures include differential privacy, synthetic data generation, and encryption, while legal frameworks strengthening data protection represent non-technical preventions.

A balanced approach combining technical innovations with safeguards, and collaboration between governments, industry stakeholders, and privacy advocates, will be a pragmatic route to ensure an ethical and responsible implementation of private connected vehicle data.

C-ITS data road users' information and potential leak impact (EO16)

The impact of processing users' personal data involves exploring the inherent risks of reidentification if leaked and the potential impact on individuals' privacy. Deanonymisation of connected vehicle data is the starkest risk. Studies consistently show that even pseudonymised or aggregated mobility datasets can be reverse engineered since just a few location data points suffice to uniquely identify individuals within large datasets.

The content transmitted of C-ITS message headers and payloads includes personal information such as vehicle location, speed, heading, etc. Correlating V2X attributes with personal data, it is possible to deduce personal information, such as home and work locations, travel habits, and real-time tracking capabilities, even uncovering daily schedules, driving behaviour, and personal preferences that may serve as unique biometric identifiers. Therefore, a structured risk assessment of privacy threats must consider attacker capabilities, attack types, and the estimated likelihood and impact. This will show that many high-impact risks arise not only from well-equipped state-level actors but also from private entities with lesser capabilities, highlighting the broad attack surface and underscoring the need for targeted mitigation strategies.

Pitfalls that increase the risk of reidentification (EO18)

In specific cases, some auxiliary information, such as aerial imagery or public datasets, could support inferences about vehicle identities. In these cases, contextual factors allow to overcome anonymity, given that the latter uses basic aggregation or pseudonymisation measures. Scenarios and examples of potential reidentification pitfalls are available, ranging from linkages between vehicle trajectories and home locations to correlations with external datasets such as tolling or mobile app usage, each illustrating how seemingly anonymised data can still be traced back to individuals when combined with sufficient auxiliary information.

Measures to prevent reidentification (EO17)

Identifiability prevention strategies must also avoid compromising the functional value (interoperability and usability) of the data. Mitigations cannot be reactive or generic, but rather proactive, especially in high-risk use cases involving longitudinal vehicle tracking or high-resolution geolocation.

Effective strategies combine technical data protections with governance safeguards and public trust mechanisms. These include technical interventions (such as reduced spatial resolution, random perturbation, or differential privacy techniques) and organisational and procedural protection controls (such as access limitations, contractual clauses, and transparency obligations).

Privacy recommendations with new use cases and data uses (EO19)

No single technique provides complete connected vehicle deanonymisation privacy protection. While pseudonymisation and geo-obfuscation are practical short-term options, their limitations in advanced threat scenarios justify a longer-term inclusion of decentralised processing and dynamic consent models.

To achieve meaningful privacy protection while ensuring interoperability and usability, a structured and phased approach is necessary. Our proposed structured roadmap reflects a phased prioritisation on the short, medium, and long terms, derived from the privacy threats, attacker profiles, and mitigation strategies. In the short term, privacy protection is based on governance and interoperability such that it can be implemented relatively quickly and easily. In the mid- and long-terms these measures are built upon enable stronger decentralisation and privacy-by-design protocols.

Subsequent reuse of data sets requires that road users trust road operators to continue using data in a lawful and deliberate manner. It is essential that road authorities strive to be open and transparent. Road authorities should understand the types of information, characteristics, behavioural patterns, etc., that can be inferred about road users from the connected vehicle data that is collected.

2.5 Expert Engagement: Workshops and Interviews

The three technical studies have been supported by independent expert engagement to collect specialist inputs. Engagement has been through online workshops and interviews.

Online workshops were held with several invited experts on 07/05/2024, 14/05/2024, 24/10/2024, 04/11/2024, and 05/11/2024. Findings from all three technical studies were presented and relevant questions discussed through breakout rooms.

The following Table 2 lists the different affiliations of the experts participating in interviews and online workshops.

Table 2: Experts participating in interviews and online workshops.

Affiliation	Role	WP
Statens vegvesen	Norwegian Public Roads Administration	WP2
Danske Vejdirektoratet	Danish Road Directorate	WP2
Horiba MIRA	UK engineering consultancy	WP2
BASt	German NRA	WP2
Eviden	EU root CA provider	WP2
Smart City Consultancy	UK consultancy	WP2
IFE	Norwegian research centre	WP2
AECOM	Irish consultancy	WP2
Wisekey Company	French consultancy	WP2
ASFiNAG	Austrian NRA	WP2,3
CAVT	UK consultancy	WP2,3
Austriatech	C-Roads Platform	WP2,3,4
Internet of Things Security Foundation	UK member body	WP2,3,4
5GAA	European association	WP2,3,4
VTT	Finish research centre	WP2,3,4
National Highways	UK NRA	WP2,3,4
Transport Infrastructure Ireland	Irish NRA	WP2,3,4
Vlaanderen	Flemish government	WP2,3,4
Vegvesen	Norwegian NRA	WP2,3,4
Trafikverket	Swedish NRA	WP2,3,4

Vayla	Finish NRA	WP2,3,4
Planet	Netherlands NRA	WP2,3,4
Applus IDIADA	Spanish consultancy	WP2,3,4
Mobilits AS	Norwegian consultancy	WP2,4
Birmingham University	UK university	WP2,4
Qfree	Finnish consultancy	WP2,4
University of Cyprus KIOS Research and Innovation Center	Cypriot university	WP2,4
Royal Holloway University of London	UK university (cybersecurity)	WP2,4
Y-mobility / AEVAC	Spanish EV association	WP3
TomTom	Mapping company	WP3
AECOM	PRESORT project coordinator	WP3
Remoted	Finish consultancy	WP3
HERE Europe	Mapping company	WP3
MAPtm	Dutch consultancy	WP3
Ljubljana University	Slovenian university	WP3
Ford	Vehicle OEM	WP3
Fintraffic	Finnish traffic management company	WP3,4
ERTICO	TISA project	WP3,4
Amey Consulting	UK consultancy	WP3,4
Microsec	Hungarian consultancy	WP3,4
Technologiestiftung Berlin	German research foundation	WP4
Imperial College London	UK university	WP4
Free University of Brussels	Belgian university	WP4
Vrije Universiteit Brussel	Citcom.ai programme	WP4
KU Leuven	Belgian university	WP4
DG Connect	European Commission	WP4
Chalmers University	CCAM Partnership Cluster 7	WP4

2.6 Deliverables and Milestones

The following Table 3 lists the TIARA project milestones and dates.

Table 3: TIARA project milestones.

No.	Name	Due Date	Actual	Status
1	KOM	11/2023	22/11/2023	Complete
2	Commencement workshop and Inception report Inception report	12/2023	20/12/2023 15/02/2024	Complete Complete
3	Expert/stakeholder workshop 1	04/2024	07/ and 14/05/2024	Complete
4	Interim report	30/06/2024	01/07/2024 (final versions 02/09/2024)	Complete
5	Expert/stakeholder workshop 2	09/2024	24/10/, 04/11/, and 05/11/2024	Complete
6	Preliminary (draft) final report	03/2025	07/04/2025	Complete
7	Final report	31/05/2025	23/06-04/07/2025	Complete
8	Final presentation at programme conference	09/2025	14/10/2025	In progress

2.7 Dissemination

TIARA's Interim and Final reports were intended for dissemination to NRAs and other road operator stakeholders:

- CEDR
- national road authorities and transport ministries in Europe
- regional road authorities and private road operators
- road vehicle OEMs (original equipment manufacturers), Tier1 subsystem manufacturers, and CAD technology developers
- standardisation bodies
- researchers, consultants and interested others.

Further external project communication was aligned with the CEDR Secretariat.

Website

A TIARA project website was created and published in cooperation with CEDR. It contains relevant information such as project description, project objectives, partners' information, contact information, and news. The website also points to CEDR's website for downloadable resources.

The website address is https://tiara.project.cedr.eu/.

Event participation

TIARA project partners participated in Transport Research Arena (TRA) conference on 15-18/04/2024, where the project was promoted informally by participants and with the project flyer alongside other CEDR materials on the TII stand. Project updates were also given informally to PEB members attending. TIARA project partners also participated in EUCAD 2024 on 19/04/2024 and EUCAD 2025 on 13-15/05/2025, where the project was also promoted informally. TIARA project partners will also participate in TRA 2026, where a paper from the project will be presented.

Abridged materials

TIARA project partners and PEB members recognised the importance of abridged materials for use within NRA organisations. These are needed to raise awareness of the challenges addressed captured in the TIARA project and the existence of the published materials from the TIARA project. The abridged materials include:

- Final programme conference presentations (10 min introduction and 30 min overview),
- Flyer (1 page with questions/prompts and links).

Flyers

The TIARA project's concept and objectives were summarised in a 2-sided A5 flyer, shown in Figure 4, which was distributed at key events including TRA2024 and EUCAD 2024. The TIARA project's findings were promoted in a 1-sided flyer as part of abridged materials, shown in Figure 5.

Figure 4: TIARA project initial flyer.

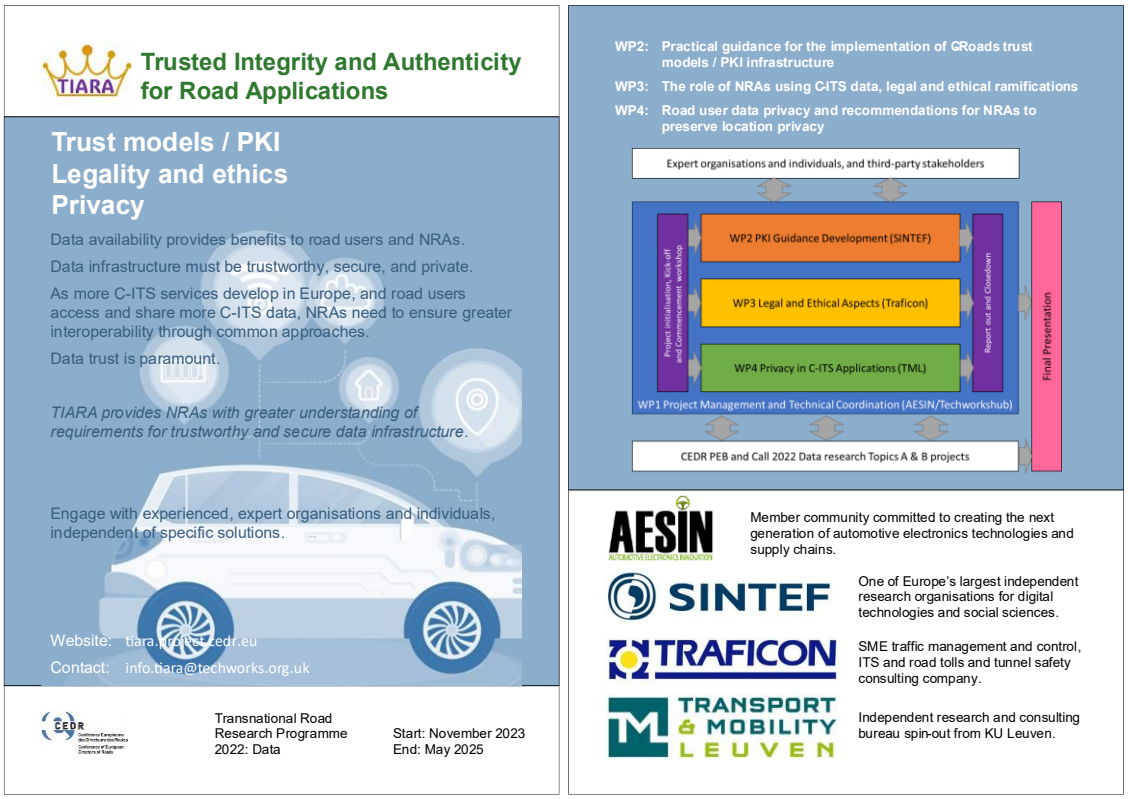

Figure 5: TIARA project final flyer.

3 References

C-Roads, 2024 ETSI, ISO CEN 2020, EC C-Roads Platform WG2 TF2 & TF3, https://www.c-roads.eu/platform.html, accessed 25/02/2025

C2C-CC, 2002 Car 2 Car Communication Consortium, https://www.car-2-car.org/, accessed 25/02/2025

CCAM, 2021 Connected, Cooperative, and Automated Mobility (CCAM) Partnership, https://www.ccam.eu/, accessed 25/02/2025

Data Ethics Framework, 2020 UK Government Data Ethics Framework: Glossary and methodology, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology, accessed 28/08/2024.

Data Quality Hub, 2021 UK Government Data Quality Framework: Guidance, https://www.gov.uk/government/publications/the-government-data-quality-framework/the-government-data-quality-framework-guidance, accessed 14/01/2025.

DROIDS, 2023 Digital Road Operator Information and Data Strategy, https://www.cedr.eu/docs/view/65a1754ac20ce-en

EU, 2008 EC recommendation on safe and efficient in-vehicle information and communication systems: update to the European Statement of Principles on HMI, 26/05/2008, https://eur-lex.europa.eu/eli/reco/2008/653/oj.

EU, 2010 EU Framework for the Deployment of ITS in the Field of Road Transport and for Interfaces with Other Modes of Transport, Directive 2010/40/EU, 07/07/2010, http://data.europa.eu/eli/dir/2010/40/oj/eng.

EU, 2024 Liability for Defective Products, Directive 2024/2853, https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng, accessed 11/06/2025.

PRESORT, 2023 Improving the use of Third-Party Data by NRAs, https://www.cedr.eu/docs/view/66855f271003b-en