Conférence Européenne
des Directeurs des Routes

Conference of European
Directors of Roads

Trusted Integrity and Authenticity for Road Applications (TIARA)

Operation of Public Key Infrastructures: State-of-the-art and best practices, and Guidance on the implementation of C-ITS PKI

Deliverable D2.1/D2.2 Version 1.0

Date 30/09/2025

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

Trusted Integrity and Authenticity for Road Applications (TIARA)

D2.1 Operation of Public Key Infrastructures: State-of-the-art and best practices, and

D2.2 Guidance on the implementation of C-ITS PKI

Due date of deliverable: 31 May 2025

Actual submission date: 01 July 2025

Start date of project:	End date of project:
22 November 2023	30 June 2025

Authors of this deliverable:

Egil Wille, SINTEF

Andrea Skytterholm, SINTEF

Per Håkon Meland, SINTEF

Table of contents

List of figures

List of tables

1 Executive summary

Digital certification is a cornerstone of trust, security, and interoperability in Cooperative Intelligent Transport Systems (C-ITS). Public Key Infrastructures (PKIs) enable secure authentication and data exchange between C-ITS stations – such as vehicles, roadside units, and traffic management systems – helping to improve road safety, traffic efficiency, and cross-border service continuity. A PKI ensures the trustworthiness of digital certificates through a defined framework of roles, policies, procedures, and secure infrastructure.

This report combines insights from a series of expert interviews and stakeholder workshops involving informants from European National Road Authorities (NRAs), industry representatives, and the provider of the EU Root Certificate Authority. While operational deployments of C-ITS PKIs remain limited, countries such as Austria and Germany have made notable progress. NRAs are expected to serve as key trust anchors within the European trust model, though much of the technical implementation will likely be delegated to specialized service providers due to the high complexity and resource demands of PKI operations.

To support a harmonized approach, the European Commission has introduced the EU C-ITS Credential Management System (EU CCMS), which defines a common trust hierarchy for certificate authorities. This report offers practical guidance on how NRAs and other stakeholders can align with the EU CCMS framework while tailoring their solutions to national and organizational contexts. The recommendations are grounded in a combination of workshop discussions, interview findings, and targeted literature review. They reflect both emerging lessons from ongoing pilot projects and insights from adjacent domains, recognizing that the formalization of C-ITS security standards was only recently finalized in 2024.

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.

2 Introduction

2.1 About TIARA

2.1.1 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.

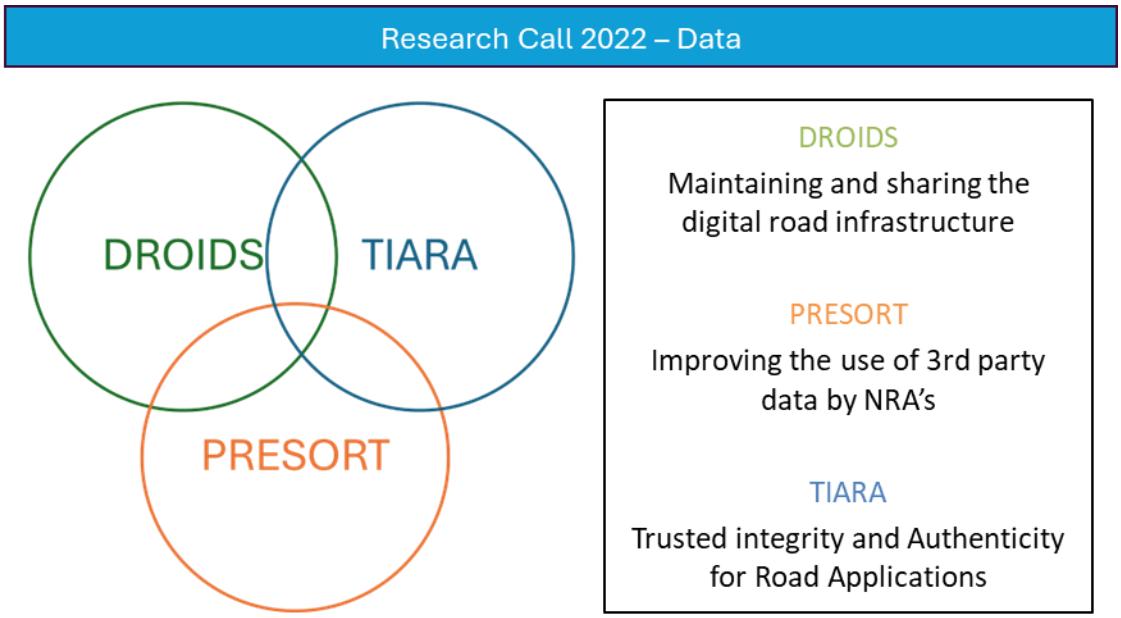

Figure 1: Three projects in the CEDR 2022 Research call on Data.

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 has been 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 that have been identified:

- Trust for C-ITS applications, to develop practical guidance for the implementation of PKI infrastructure 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 have 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.

2.1.2 European 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 Public Key Infrastructure (PKI), is the European Union C-ITS Security 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).

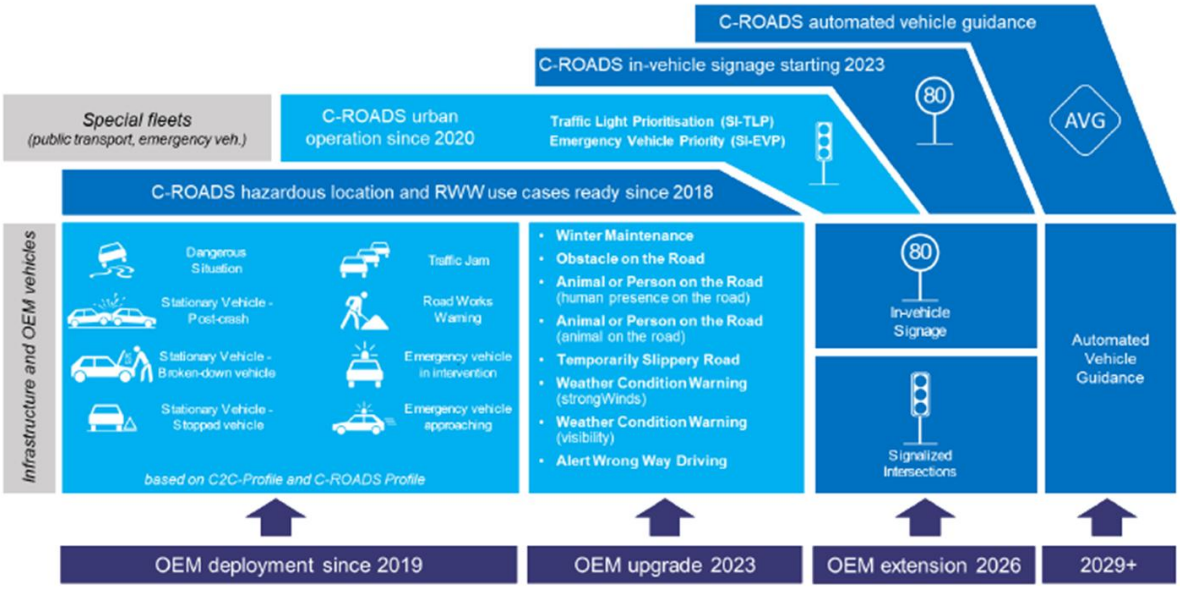

Figure 2: The C-Roads Platform for harmonisation of C-ITS deployment.

2.1.3 European 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 infrastructure

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.

2.1.4 TIARA 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.

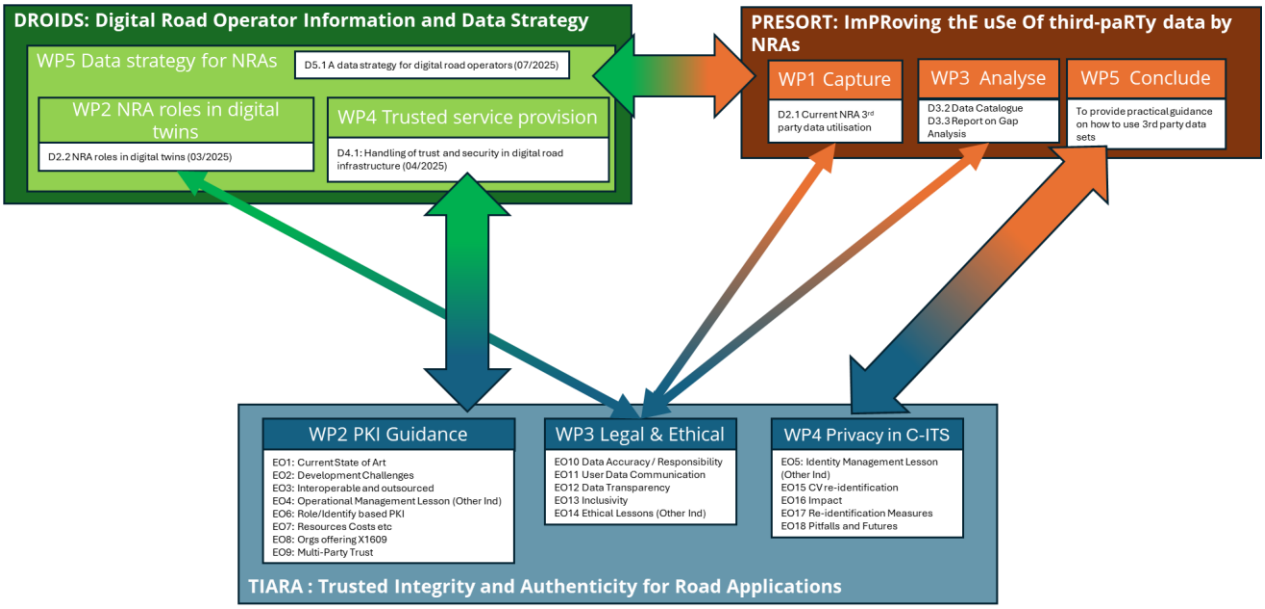

Figure 3: Linkages between scopes of the three CEDR research projects.

2.2 Study Scope

This document presents the work that has been done in WP2 of the TIARA project. The work has previously been documented in two different reports: Deliverable 2.1 “Operation of Public Key Infrastructures: State-of-the-art and best practices”, and Deliverable 2.2 “Guidance on the implementation of the C-ITS PKI”, which are summarised below. In this document, we have combined these two deliverables into one single document, to facilitate easier access to the complete results from WP2 through a single document.

2.2.1 Deliverable 2.1

The primary purpose of Deliverable 2.1 “Operation of Public Key Infrastructures: State-of-the-art and best practices” is to provide a comprehensive overview of the ongoing roll-out of the C-ITS PKI within the European NRAs. In addition, this document offers an overview of both commercial entities and public organisations that are currently providing “X.1609 PKI” functionality. This information is crucial for stakeholders interested in the broader adoption and application of C-ITS PKI technology. Finally, this document presents lessons learned from the operation of PKI and identity governance in other adjacent sectors. These lessons provide valuable insights and best practices that can guide future implementations and operations of PKI systems.

2.2.2 Deliverable 2.2

The purpose of Deliverable 2.2 “Guidance on the implementation of the C-ITS PKI” is to provide guidance for the European NRAs for the implementation of a nationwide Public Key Infrastructure (PKI) that is interoperable within Europe. It provides a practical guidance to the

NRAs on how to proceed with the implementation of the C-ITS PKI, including a roadmap with clearly identified phases and milestones to be completed.

Deliverable 2.2 builds on the findings presented in Deliverable 2.1 Operation of Public Key Infrastructures: State-of-the-art and best practices.

Deliverable 2.2 includes advice on how to build the organisations required to run a nationwide PKI that is interoperable within Europe, including guidance on the use of role-based and identity-based PKI systems. Additionally, we provide advice for developing PKI systems that provide trust across multiple parties, including the possibility to outsource (parts of) the PKI services. The main outcome of this report is a practical guidance for the NRAs on how to proceed with the implementation of C-ITS PKI, including a roadmap with clearly indicated phases and milestones to be completed.

The roadmap is developed based on input from informants gathered through interviews and workshops. We have also incorporated experiences from other domains, as presented in D2.1 (see section 5.3), and from relevant sources such as the UK National Cyber Security Centre (NCSC).

2.2.3 Expected outcomes

The table below summarises the expected outcomes of WP2 of the TIARA project. The rightmost column indicates where in this document the results have been documented.

Table 1: Expected Outcomes in WP2

#	Description	Reference
EO1	Review of the current stake of PKI roll-out in European NRAs (State of the art)	Sections 5 and 6
EO2	Analysis of the issues and problems that NRAs will encounter when developing PKI infrastructure.	Section 7
EO3	Advice for building the organisations required to run a nationwide PKI infrastructure that is interoperable with Europe, and advice on outsourcing PKI services.	Section 7
EO4	Lessons from other industries (finance, healthcare, etc.) on operation of a PKI infrastructure.	Sections 5 and 6
EO5	Lessons from other industries (license plate registry, etc.) on governing of identities.	This topic is related to GDPR and personal data, and is addressed in WP4.
EO6	Guidance on the use of role-based and identity-based PKI.	Section 7

EO7	Analysis resources required to run C-Roads PKI infrastructure, including how the cost and computational requirements scale, and the administration required for certificate and key management.	Section 7
EO8	View of commercial and public organisations offering X.1609[1] PKI functionality	Sections 5 and 6
EO9	Advice for developing PKI systems that provide trust across multiple parties, for example extending the trust infrastructure to road workers or maintenance companies.	Section 7

2.3 Structure of this document

This document is structured according to the table below

Section	Description
3 - Background	Provides the background for the deliverable and introduces relevant C-ITS initiatives and organisations
4 - Methodology	Presents the methodology used
5 - D2.1 Findings	Presents findings from the first phase of WP2
6 - D2.1 Conclusions	Conclusions from the first phase of WP2
7 - D2.2 Findings and guidance	Presents findings from the second phase of WP2, including a roadmap with phases and milestones to be completed
8 - D2.2 Conclusions	Conclusions from the second phase of WP2, including implementation guidance
Appendices	This section contains supplementary material that is relevant to the main text but not essential to its core arguments

[1] We assume that "X.1609" is a typing error (a mistaken combination of X.509 and 1609.2), and that it should say "1609.2" instead

2.4 Acronyms

AA	Authorisation Authority
ACARS	Aircraft Communications Addressing and Reporting System
ARINC	Aeronautical Radio, Incorporated
ATA	Air Transportation Association
ATM	Air Traffic Management
C2C-CC	Car 2 Car Communication Consortium
CA	Certificate Authority
CDMA	Code-Division Multiple Access
CEDR	Conference of European Directors of Roads
CEO	Chief Executive Officer
C-ITS	Cooperative Intelligent Transport Systems
CL-PKC	Certificateless-Public Key Cryptography
CPA	Certificate Policy Authority
CPOC	C-ITS Point of Contact
CRL	Certificate Revocation List
DG MOVE	Directorate-General for Mobility and Transport
DoRN	Description of Research Needs
DSRC	Dedicated Short-Range Communication
EA	Enrolment Authority
EC	European Commission
ECTL	European Certificate Trust List
eIDAS	electronic IDentification And trust Services
ENCAP	The European New Car Assessment Programme
ETSI	European Telecommunications Standards Institute
EU	European Union
EU CCMS	EU C-ITS Security Credential Management System

EUDI	European Digital Identity
GmbH	Gesellschaft mit beschränkter Haftung (company with limited liability)
GSM	Global System for Mobile Communications
IBC	Identity-Based Cryptography
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet-of-Things
ITS	Intelligent Transport Systems
LTE	Long-Term Evolution
NAP	National Access Point
NRA	National Road Authority
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OPEX	Operational Expence
PEB	Programme Executive Board
PKI	Public Key Infrastructure
PSID	Provider Service Identifier
RCA	Root Certification Authority [remove, and stick to "Root CA"?]
RSU	Roadside Unit
RTTI	Real-Time Traffic Information
SRTI	Safety-Related Traffic Information
SSP	Service Specific Permissions
TIARA	Trusted Integrity and Authenticity for Road Applications
TLM	Trust List Manager
TLS	Transport Layer Security
TRA	Transport Research Arena
V2I	Vehicle-to-Infrastructure

V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VW	Volkswagen
WP	Work package

3 Background

3.1 Relevant C-ITS initiatives and organisations

The following sections present a selection of the most relevant initiatives and organisations, along with relevant documents for communication and information security in European C-ITS systems.

3.1.1 C-Roads

The C-Roads Platform is a cooperation of member states and road operators, working towards harmonized and interoperable C-ITS services in Europe. C-Roads is co-funded by the European Union.

The main goals are to link C-ITS deployment across Europe, to develop, share and publish common technical specifications, and to test and verify interoperability between deployments and nations. These efforts aim to enable coherent C-ITS deployment in European Union, for both long-term and large-scale roll-outs.

The C-Roads steering committee consists of representatives from the member states and infrastructure operators, and provides an interface to all internal and external stakeholders. The steering committee receives decision support from various working groups and task forces. The C-Roads organisational and operational structure is illustrated in Figure 4.

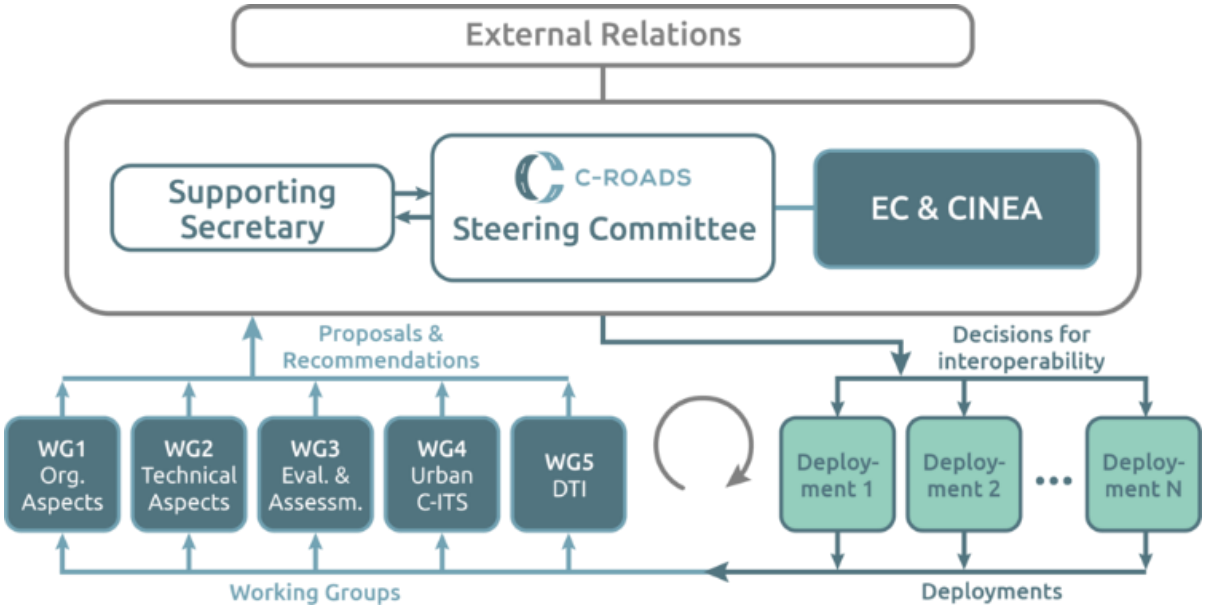

Figure 4: C-Roads organisation and operation (https://www.c-roads.eu/platform/about/about.html)

More information, including various relevant reports and other documents, can be found on the C-Roads homepage (https://www.c-roads.eu/platform.html).

3.1.2 Car 2 Car Communication Consortium (C2C-CC)

The CAR 2 CAR Communication Consortium is a group of vehicles manufacturers, equipment suppliers, engineering companies, road operators and research institutions which have joined forces to enhance road safety and traffic efficiency through research and development of C-ITS solutions. Their work focuses on interoperability across vehicle classes and borders, leveraging V2X communication for safer, cooperative driving.

C2C-CC was founded in 2002 and aims for global standardisation and the promotion of C-ITS to achieve a vision of zero road accidents. The C2C-CC organisational structure is illustrated in Figure 5.

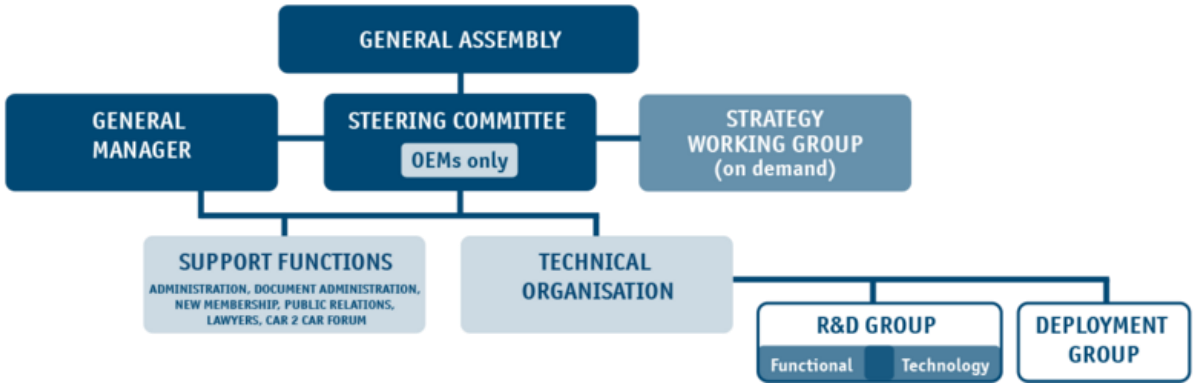

Figure 5: C2C-CC structure

More information can be found on the C2C-CC homepage (https://www.c-roads.eu/platform.html).

3.1.3 NAPCORE

NAPCORE (National Access Point Coordination Organisation for Europe) is an initiative aimed at harmonizing mobility data across Europe. It was established in response to the ITS Directive 2010/40/EU, which mandates that each European Member State must set up a National Access Point (NAP) for mobility data. These NAPs serve as repositories where mobility-related data is published and made accessible, primarily for use in travel information services. The NAPCORE project seeks to improve the interoperability of these NAPs, ensuring consistent and coordinated access to mobility data used for travel information services. NAPCORE is co-funded by the European Union.

More information can be found on the NAPCORE website (https://napcore.eu/)

3.1.4 EU CCMS

The European Union C-ITS Security Credential Management System (EU CCMS) is a framework set up by the European Commission. It relies mostly on two main documents[2], the Certificate policy (Joint Research Centre, 2024) and the Security policy (Joint Research Centre, 2023).

[2] Updated versions of the EU CCMS policy documents can be found at https://cpoc.jrc.ec.europa.eu/Documentation.html

The European Commission aims to offer support for European C-ITS deployment with three different levels of TLM services. The first level, L0, is used for testing and pilot purposes. L1 is the intermediate level, where stations and use cases are in operation, but with some exceptions regarding regulations. The final level is L2, and here the stations and use cases need to be fully compliant with the regulation. L0 only requires a self-declaration, whereas L1 and L2 entail a regulation assurance process.

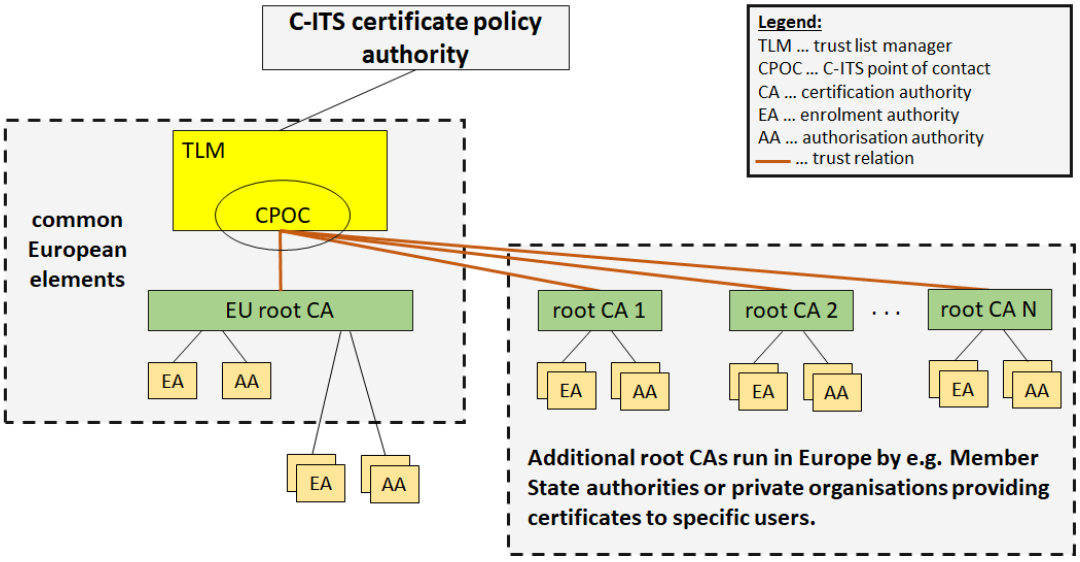

Figure 6: C-ITS Trust model architecture (Joint Research Centre, 2024)

3.1.5 ETSI

The European Telecommunications Standards Institute (ETSI) is an independent standardization organization focused on the telecommunications sector. Established in 1988, ETSI is involved in the development and testing of technical standards for ICT systems and services globally. Recognized by the European Union as a European Standards Organization, ETSI's work supports EU regulations and policies through the creation of harmonized standards.

In addition to working with mobile communications such as 3G, 4G and 5G, ETSI has also developed what is commonly referred to as the "ITS-G5" standard which is highly relevant for short-range C-ITS communications. The ITS-G5 standard is using already existing standards for communications, and the document that defines the access layer technology for ITS-G5 (ETSI, 2020) refers to several specifications and standards from IEEE and ETSI.

When discussing technical standards such as those defined by ETSI, it is also relevant to mention standardization bodies such as ISO, IEC and SAE. In this context, however, the ITS-G5 standard has received particular attention, and we have therefore highlighted ETSI. A more comprehensive overview of safety, security and privacy standards can be found in deliverable D10.2(Shan, 2019) of the SECREDAS project, funded by the EU's Horizon 2020 programme.

More information can be found on the ETSI home page (https://www.etsi.org/)

4 Methodology

This report presents our findings gathered from multiple interviews and workshops conducted with domain experts, and a literature study of PKI operations from other sectors.

4.1 Interviews

Interviews have been conducted with various C-ITS personnel, mainly from European NRAs. In total, 8 interviews with 12 domain experts were conducted. The interviewed experts were selected based on a contact list including NRAs, PEB members, and individual experts. The list has been populated by project participants, and also extended and approved by PEB members. We refer to these interviewees as *informants*, since they have *"specialist knowledge about other people, processes or happenings that is more extensive, detailed or privileged than ordinary people, and who are therefore particularly valuable sources of information to a researcher"* (Payne & Payne, 2004). The informants have provided information from countries with varying maturity levels on C-ITS PKI deployment, and we therefore consider our findings to be relevant for the whole Europe.

The interviews were semi-structured, allowing for open discussions and giving the informants the opportunity to address topics or questions not raised by the interviewers. The interview guide can be found in Appendix A and an overview of the affiliations and roles can be found in Table 2.

Table 2: Overview of interviewees

Organisation role	Affiliation	Informant roles
NRA for Norway	The Norwegian Public Roads Administration (Statens vegvesen)	• Senior engineer • Solution architect • Senior engineer
NRA for Denmark	Danish Road Directorate (Danske Vejdirektoratet)	• Special consultant
Consultancy company based in Norway	Mobilits AS	• CEO/consultant
Automotive engineering and development consultancy company based in the UK	Horiba Mira	• Senior Functional Safety/ Cyber Security Engineer
NRA for Germany	BASt	• (Dipl.-Phys) Research Assistant
NRA for Austria	ASFiNAG	• Expert in Cooperative, Connected and Automated Driving
EU Root CA provider, based in France	Eviden	• Head of Engineering

		• V2X & IoT Security Business Manager
NRA for Flanders	Agentschap Wegen en Verkeer (Flemish Agency for Roads and Traffic)	• C-ITS ecosystem expert • Expert C-ITS and CCAM

All interviews were recorded and automatically transcribed. The recording and automatic transcription was done using the Microsoft Teams recording and transcription functionality. All informants have signed a consent form, informing them about how the data will be processed and stored during the project, and what will happen with the data after the project ends. All informants have also given their consent to include their affiliation and role/title in the report.

When post-processing the automatically generated interview transcripts, AI chatbots (Microsoft Copilot and Open AI's Chat GPT) were used to generate summaries and identify main topics (using queries such as "based on the following interview transcript, please write a summary of the interview and highlight the main topics which were discussed" and "what were [interviewee]'s opinions on the matters discussed?"). To prevent unwanted use and sharing of the interview transcripts, only paid subscriptions were used to access the mentioned AI chatbots. Due to text length limitations in the query fields, the interview transcripts were split into parts before they were shared with the chatbots. The summaries and thematic overviews generated were then used in combination with the transcripts and human-written notes to extract the main findings, which are summarised in section 5.

4.2 Workshops

In addition to the interviews, four expert workshops were held. In total, 26 informants participated in the workshops, along with 8 representatives from the project. Among the informants were mainly NRA representatives, consultants, researchers and representatives from different ITS stakeholder organizations. Both expert workshops started with an introduction to the TIARA project, followed by a summary of all work packages and the initial findings. After that the informants were divided into two break-out sessions based on their interests and competence, and one of those sessions covered the C-ITS PKI topic of WP2. A total of 12 informants participated in the PKI breakout sessions.

The goal of the workshops was to present our initial findings, and to get more information on specific topics based on our previous findings. An interactive workspace for collaborative work, or a virtual whiteboard, was used in the workshop to present the discussion topics and allow informants to write down their input. When facilitating the discussion, we also ensured to write down the points that were not already written down.

The data from the workshops have been analysed and are presented in section 5.

4.3 Literature study

We believe that many sectors have faced many of the same challenges of PKI operations as C-ITS. Hence, we conducted a study of academic literature and publicly available reports on lessons learned on a selected set of sectors. The sources were identified using a combination of traditional keyword search (such as “PKI” + “lessons learned” + [SECTOR]) using Google Scholar, and Microsoft Copilot, which is an AI companion that combine technology such as GPT-4 and Bing (using queries such as “what are the lessons learned from academic literature on operating a PKI in the [ZZZ] sector?”). The sources were filtered, read and synthesized according to relevance by human researchers. The results are presented in section 5.3.

5 D2.1 Findings

Since the identified and available literature provides insufficient information for answering the DoRN questions related to C-ITS PKI, the majority of this report is based on input from interviews and workshops with relevant C-ITS actors (including representatives from various European road authorities).

The following subchapters present findings from the interviews and workshops, as well as a summary of lessons learned from PKI operations in other sectors.

5.1 Interviews

5.1.1 Germany

Our informant from Germany comes from the *Federal Highway Research Institute* (BASt, *Bundesanstalt für Straßenwesen*) in Germany. BASt is a part of the Ministry of Transport, and are involved in standardisation, contribute to regulation and are actively involved in research projects related to C-ITS.

The informant explained that in Germany, the first operational deployment of a federal Root CA has been the responsibility of the Autobahn GmbH, which has been used for piloting e.g. services for road work warning trailers. This PKI is offered to other parties as well, but with some limitations. Currently, Autobahn GmbH is financing the root CA on behalf of the public bodies. They are also closely aligned with their Austrian counterpart. There are also examples of more local pilot sites that operate their own PKI, such as in the city of Hamburg. Both Autobahn GmbH and the city of Hamburg have contracted private companies to operate their PKIs. Though this is the current situation, Germany is still figuring out what the long-term PKI structure should be. There is an ongoing analysis looking at the needs in terms of the number of road stations, number of different services and number of different actors that need to be registered in the PKI.

The informant's further opinions can be summarized around the following key points:

- **PKI implementation challenges**: The informant acknowledges the complexities and challenges of implementing and managing PKI systems, particularly in terms of regulatory and operational requirements. He recognizes that managing a PKI system requires strict processes and significant expertise, which are often challenging to maintain consistently over time.

- **National vs. European PKI**: The informant discusses the advantages and disadvantages of maintaining a national PKI system versus using a European-wide system. The informant suggests that while a national system offers more control and customization, a European system could be more cost-effective and reduce redundancies across member states. Also, in Germany, there are 16 federal states that operate more or less independently. These could set up their own PKIs, but that would probably not be very efficient. Related to financing, the national level would not be paying for several PKI infrastructures in the individual federal states. The Federal Office for Information Security in Germany have created a set of national guidance documents

and argue for a national root CA rather than at EU level in order to be independent of other actors and able to modify the PKI if considered necessary.

- **Cross-border data sharing**: The informant is supportive of enhanced data sharing capabilities across borders within the C-ITS framework, acknowledging the technical potential and the benefits of interoperability. A concrete example is that the Austrian road operator can subscribe to German the information stream on road work for certain corridors close to the border and vice versa, thereby improving cross-border traffic management. However, he also notes the current limitations and the need for improvements in system integration.

- **Technological challenges**: The informant expresses concerns about the impact of patents and proprietary technologies on the accessibility and cost of communication technologies, particularly how these might affect the broader deployment of C-ITS technologies.

- **Workforce and expertise**: The informant is candid about the difficulties in finding and retaining the right talent to manage a PKI system. He stresses the niche nature of the expertise required, which is not commonly taught in traditional educational settings, making it a significant bottleneck.

- **Future regulations and standards**: The informant is optimistic about the future developments in regulations and standards, particularly those being considered by the European Commission, since a very stable basis has already been established. The informant hopes for a more streamlined and integrated approach to C-ITS security, ideally simplifying the current complex landscape.

- **Collaboration and knowledge sharing**: Throughout the interview, the informant advocates for greater collaboration and knowledge sharing among countries and experts in the field. He believes that learning from each other's experiences and challenges can lead to more effective and efficient PKI and C-ITS implementations.

All in all, the informant’s opinions reflect a thoughtful consideration of the operational, technical, and strategic challenges involved in PKI and C-ITS. He emphasizes the need for adaptability, collaboration, and expert knowledge to navigate the evolving landscape of transportation technology and infrastructure security.

5.1.2 Austria

Our informant from Austria is an expert in cooperative, connected and automated driving, representing ASFiNAG.

Austria is one of the early adopters of C-ITS and the country that has come the furthest with regards to deployment of operative C-ITS stations. For them, it is therefore paramount to have a safe and secure system that people trust.

ASFiNAG is a roadside operator and therefore does not have a high number of C-ITS units compared to vehicle original equipment manufacturers (OEMs). Thus, establishing their own

PKI was not deemed as the most practical or cost-effective solution. The possible solutions at hand were the following: the first option was to go with the EU Root CA, which is financed by the European Commission. The second option was to use the existing PKI of another operator, and the third option was to operate their own PKI. They decided to use an existing PKI solution for the start of operations.

To have an operational system, they needed to be able to reach their users/customers inside the cars. This required a common trust with the OEM that is deploying this kind of technology, and in 2019 when the decision was made, Volkswagen was the only OEM that had the technology built into operational vehicles. Volkswagen then granted them access to one of their own project PKIs, which has a direct bilateral trust with their vehicles. By using this PKI, their messages are displayed in operational vehicles.

In the process of selecting which communication protocol to use, Austria has chosen the short-range communication protocol, ITS-G5. ITS-G5 has undergone extensive testing and is considered a stable solution. When implementing the system inside vehicles that are operational for 10 years or more, it is important that the solution is stable and does not change for the lifetime of the vehicle.

The C-ITS messages sent from their stations are broadcast and sent to any receiver in the area using ITS-G5. The messages are signed using the PKI offered by Volkswagen, so anyone that trusts this PKI can receive and validate them. However, currently there are no other OEMs than the Volkswagen group that have deployed C-ITS in their vehicles.

In the future, the goal is to be part of the European credential management system so that everybody can trust each other. They are considering partnering up with the German Autobahn GmbH and make use of their PKI. Today, it does not make any sense to go onto the EU Root CA under the European Certificate Trust List (ECTL) level 1 (L1) if they are there alone and then their messages are completely secure, but these are not processed and displayed because they are not trusted by the receiving systems. Therefore, in the near future, the goal is to be part of the European credential management system either using the German "Autobahn GmbH" PKI or preferably the EU Root CA, so that everybody can trust each other.

Austria has had quite a lot of research projects with the industry, more information about such projects can be found in the C-Roads pilot overview report (C-Roads, 2023). These projects have allowed for testing of the system and building up specifications which further were used for the tendering system. They received high maturity of the specifications of the solutions offered by the industry through all those years of running those projects.

The informant's further opinions can be summarized around the following key points:

- **C-ITS deployment:** The informant believes that Austria’s early adoption and deployment of C-ITS have positioned the country as a pioneer in this field. He emphasizes the importance of operational systems and the need for high-quality, timely, and geolocated data about road events.
- **PKI implementation:** The informant supports the decision not to operate Austria’s own PKI, instead opting to use Volkswagen’s PKI and partnering with the German Autobahn GmbH. He sees this as a practical and efficient solution given the low number of certificates required by their roadside units.

- **EU trust Model:** The informant is hopeful about the move to the EU trust model in the near future, which would allow all systems to trust each other. However, he acknowledges that this would require concerted action where multiple parties move to the EU trust model together at the same time.
- **Challenges:** The informant acknowledges the challenges faced during implementation, particularly the need for high-quality, timely, and geolocated data about events on the roads. The informant sees the digitalization of this information as a significant task that goes beyond C-ITS.
- **Future plans:** The informant hopes that more OEMs will start deploying CITS in their vehicles, which would necessitate a move to the EU trust system. He also hopes that Volkswagen Group will move to the EU trust system in the near future.
- **Communication technologies:** The informant supports Austria's strategy to deploy C-ITS based on ITS-G5, a short-range communication based on Wi-Fi. The informant believes this technology is stable enough to be deployed in vehicles and is expected to be operational for at least 10 years.
- **National and European projects:** The informant values the importance of Austria's involvement in various research projects and field tests to develop and refine the specifications for C-ITS. The informant believes these specifications form the basis for the future C-ITS delegated act.
- **Trust model:** The informant supports the European trust model developed to allow for multiple root CAs while maintaining trust across all systems. The informant sees this model as a practical solution that respects the sovereignty of Member States in Europe.
- **Quality of information:** The informant emphasizes the importance of providing high-quality information to users. He believes that both false positives and false negatives can erode user trust in the system, and therefore, maintaining the quality of information is crucial.

In summary, the informant's opinions reflect a pragmatic and forward-thinking approach to the implementation of C-ITS and PKI in Austria. He acknowledges the challenges but also sees the potential benefits and future possibilities of these technologies. He emphasizes the importance of cooperation, high-quality data, and user trust throughout the conversation.

5.1.3 Denmark

Our informant from Danmark is a coordinator in the traffic center of the Danish Road Directorate.

Denmark currently does not have a C-ITS deployment decision nor a deployment strategy. Recently, they have decided to go ahead with a very small demonstration project with the implementation of two use cases. The first use case is road works warning (RWW) demonstrating static roadworks warnings at the E45 in Jutland. The second use case is emergency vehicle interventions (EVI) and emergency vehicle approaching (EVA). Their greatest barriers are the PKI, the software systems, data flow, working processes, operational set-up and managing the roadside units.

Denmark is currently in the process of considering "PKI as a service". The likely goal is to be able to operate some of the systems from the Danish Road Directorate., The intention is for

the Danish Road Directorate to act as the enrolment authority and the authentication authority. However, they have not taken a formal stand about if and how to move along with C-ITS. They are preparing a decision basis for the management to be presented by the end of 2024.

They understand that there is a bit of competition between short-range and long-range communication standards, and therefore the informant believes they will go for a hybrid solution where both standards will be used. The informant also believes there will be parallel PKI systems for different kinds of services.

The informant mentioned that it is difficult for them to get funding and make a choice when things are not set in stone, and they are therefore waiting for things to be ready, among others from the EU side. They are waiting for more information on how the implementations should work in the optimal set-up and how to ensure interoperability in a European context.

Another reason for holding back is that the solutions are still expensive, and the informant said that they expect that this will be much cheaper in just a year's time or so. Today there are not many vendors selling the hardware and software solutions needed, and they expect that more vendors will come into the market as has been seen with ITS equipment in general. They are aware that the solution will cost money, but they accept the costs if it can balance the investment in relation to safety out on the road. Now they must prove that the solution is safe and that it provides safety for their colleagues working on the roads and for the road users.

Denmark collaborates with other European countries as part of the C-Roads platform and was also a partner in the NordicWay projects[3], where NordicWay3 finished by the end of 2023. The NordicWay project had a lot of sub-groups working on different topics, and one of the groups worked with security and certifications. Additionally, Denmark is part of the National Access Point Cooperation (NAPCORE), where they are working on e.g., the interchange solutions between the national access points.

The informant's further opinions can be summarized around the following key points:

- **C-ITS implementation in Denmark:**
  - Denmark focuses on safety, data quality, and collaboration with other countries.
  - Denmark aims to provide traffic information via a hybrid approach using both long-range and short-range communication where relevant.
  - Use cases include emergency interventions incl. emergency vehicle approaching, and road works, incl. static road work warnings.
  - Challenges include PKI implementation and balancing technology excitement with safety considerations.
- **Collaboration and data sharing:**
  - Denmark collaborates with C-Roads and NAPCORE; and further with Nordic countries and Germany on C-ITS.
  - NAPCORE focuses on coordination and harmonization of mobility data platforms in Europe, including interchange solutions for sharing data between national access points.
- **Data quality:**

[3] https://www.nordicway.net/

    - Denmark wants to ensure safe implementations and small-scale demonstrations before widespread adoption.
- **Political considerations and funding:**
    - Denmark has not yet formally presented C-ITS decisions to top management or politicians.
    - Funding challenges exist, but a common European vision is crucial for success.
- **Future directions:**
    - Balancing technology rollout with safety and scalability is essential.
- **Challenges and excitement:**
    - Denmark faces challenges related to manpower, communication, system and organizational integration, governance, and political support.
    - The team is excited about making C-ITS information available and ensuring safety.

Overall, Denmark's cautious optimism and commitment to safety provide valuable insights for ongoing CITS research and implementation efforts.

5.1.4 UK

Our informant from the UK is a chief engineer for cybersecurity at Horiba Mira which is a consultancy and test service company delivering services for the automotive industry.

Horiba Mira have been involved in collaborative programs within the UK on C-ITS pilots. They are waiting to see whether C-ITS will be adopted in the real world, and starts to become fitted to vehicles, however, this seems to be a little way in the future.

They have observed some challenges around which technologies to be adopted, and it is still unclear whether the ITS-G5 or the cellular V2X solution will be the preferred solution in Europe. Another challenge is the monetization of the application, and who will benefit and who will pay for these kinds of services, and this is probably the most challenging part. The informant believes that the UK will go for a hybrid solution with a combination of ITS-G5 and V2X, but that this also could make it more challenging for implementers.

The informant expects that the PKI solution will be outsourced to a subcontractor responsible for implementation and operation, but he also assumes that the UK government will be the owner of the solution, however, no official announcements have been made.

The informants' further comments are summarised in the following key points:

- **Introduction to C-ITS:**
    - C-ITS involve direct communication between vehicles and road infrastructure.
    - Goals include enhancing road safety, improving traffic flow, and providing real-time information to drivers.
    - Services cover various aspects, including traffic management, emergency response, and driver assistance.
- **European Commission's Strategy:**
    - The European Commission adopted the C-ITS strategy in 2016.

    - Aims to align investments and regulatory frameworks across EU member states.
    - Mature C-ITS services were expected to roll out from 2019 onward.
    - Legal Frameworks are necessary for harmonization and interoperability of the services.
    - EU Funding to support research, development, and deployment of C-ITS services.
    - The European Commission encourages collaboration across countries and regions.
- **Responsible Organizations:**
    - UK Department for Transport:
        - Responsible for C-ITS matters in the UK.
        - Collaboration with the National Cybersecurity Centre ensures security aspects of the C-ITS.
        - National Highways (operating motorways and major roads) may also play a role.
- **Challenges:**
    - Interoperability: Ensuring seamless communication across different systems and brands.
    - Cross-Border Information Exchange: Managing transitions between different PKIs (Public Key Infrastructures) when vehicles cross borders.
    - Security: Balancing robustness with security measures.
    - Political Barriers: Differing views and priorities among stakeholders.
- **Trials and Practical Experience:**
    - Most practical experiences are related to trials rather than full-scale operations.
    - Trials focus on functionality but often overlook security aspects.
    - Questions remain about the need for continuous trials and bridging gaps.
    - Security Considerations:
        - Security should be a significant focus in future trials.
        - Ensuring robustness while maintaining interoperability is critical.
- **Future Directions and Research:**
    - Need for standardized use cases and message formats.
    - Questions about how different PKIs interact internationally.
    - Consider more continuous field trials beyond isolated events.
    - Explore long-term deployment challenges.
    - Investigate sharing information across vehicle brands and national boundaries.
    - Address privacy concerns and anonymization of data.

In conclusion, C-ITS faces multifaceted challenges, but efforts continue to advance this transformative technology across Europe. The need for collaboration, standardization, and security remains paramount.

5.1.5 Norway

Two different Norwegian C-ITS stakeholders were interviewed. In the first interview, the Norwegian Public Roads Administration participated with 3 representatives, and in the second, a C-ITS consultant participated on behalf of his company Mobilits AS.

5.1.5.1 The Norwegian Public Roads Administration

Regarding PKI rollout and ongoing initiatives, we were told that there is very little C-ITS hardware in the Norwegian road infrastructure. The Norwegian Public Roads Administration currently has three mobile radio devices. On the vehicles side, Volkswagen (VW) has come a long way compared to other manufacturers and delivers all their new cars with C-ITS capability built in. Until recently, however, radios from VW were geofenced and inoperable in Norway. Although Norway currently lacks operational C-ITS services, there have been some work and discussions regarding safety related applications and smart traffic lights. Traffic safety implementations are of particular interest.

When discussing the technology, two main types of C-ITS communication were mentioned, namely ITS-G5 which is a short range (essentially Wi-Fi) communication, and an ad hoc version of cellular communication commonly referred to as C-V2X. Each has certain advantages over the other and the choice of communication technology depends on the use case and other factors. The informants expect to see both technologies being widely used within C-ITS, so the service providers will need good solutions for how these technologies should coexist and interact in the C-ITS domain. The complementary use of ITS-G5 and C-V2X is commonly referred to as hybrid communication, and many countries now seem to opt for such a solution. Even Austria, which has been a significant ITS-G5 advocate, has shown interest in hybrid communication.

Several car manufacturers have chosen C-V2X communication for their vehicles, while others, such as VW, have chosen ITS-G5. There is an ongoing "competition" between the two approaches, where the final outcome is still undecided. The lack of a widely adopted solution is considered a barrier for C-ITS implementation, as it makes various stakeholders (such as infrastructure providers) reluctant to invest in solutions whose relevance is still uncertain.

The informants are currently aware of one C-ITS PKI for Norwegian services, which is provided by TeskaLabs[4] and included in the ECTL. This was developed under the C-ITS delegated act[5] and has been refined and modified in recent years. The delegated act was not approved.

Regarding data sharing and traffic safety, it was mentioned that different car manufacturers currently do not share data from each other's vehicles, but there is sharing of data within each manufacturer's "fleet". The ITS directive[6] encourages more sharing (to improve safety), but such sharing is not required.

The interviewees envision that Norway will have its own root CA in the EU CCMS trust hierarchy in the future. This will require resources (either in-house or outsourced) to manage

[4] https://teskalabs.com/
[5] https://www.europarl.europa.eu/cmsdata/161226/Delegated%20Regulation%20C-ITS.pdf
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010L0040

policies, enrollment, etc. In such a system there can be different types of users, e.g. police cars, ambulances, maintenance vehicles, repair shops, etc.

The informants did not have specific opinions regarding certificate validity and revocation in C-ITS, as there has so far been very little discussion on these topics in their organization. The choice of validity management (revocation or short-lived certificates) will depend on the type of application/service.

The Norwegian Public Roads Administration currently has very little experience with costs related to PKI operations, but the interviewees expect that there will be significant costs related to operation (OPEX), including support, maintenance and certificate management). Any functionality or service which utilizes wireless communication will have to be included and managed.

Regarding the way forward, the informants have the impression that several of the applicable standards are not sufficiently understood and applied, such that there is currently a "learning phase" among many C-ITS actors. There is a concern that we will see an "over-engineering phase" before the application of the standards has "normalized". As with various other services, there is a need to move from a "shell-based" protection approach to a transaction-based system, and this applies to the entire value chain.

The Norwegian Public Roads Administration is eager to learn from the experiences of other NRAs (and vice versa). As specific partners/sources, Denmark and the Netherlands were mentioned. The informants believe in small and agile initiatives, to allow "failing fast" and identifying pitfalls such that the consequences of failures and bad choices are minimized while the technology matures.

5.1.5.2 Mobilits

To provide a bit of history/background, Mobilits mentioned the Directorate-General for Mobility and Transport (DG MOVE)[7] early in the interview. DG MOVE was created in 2010, and their work with cyber security for C-ITS has played and still plays a big role when it comes to topics discussed in this project. In the early stages (from 2013-2014), C-ITS was "synonymous" with short range car-to-car communication.

For short range C-ITS communication (commonly referred to as ITS-G5), IEEE p1609.2[8] is the main certificate standard. To address privacy issues in automotive applications, pseudonymous certificates is a common approach. In today's C-ITS services (which are mostly safety related), a lot of data is broadcast openly, but anonymously, from C-ITS enabled vehicles. These messages have no confidentiality, only anonymity and integrity (via signatures and certificates). According to the informant, there are currently about 15000 to 20000 such cars in Norway, using 1609.2 certificates. The majority of these are from VW.

At present, only VW has a significant number of operational cars with p1609.2 capabilities. Among road operators, there are a few which have rolled out a significant number of roadside

[7] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/mobility-and-transport_en
[8] https://standards.ieee.org/ieee/1609.2/10258/

stations, most notably Austria. There are also many roadside and mobile work zone stations along the German Autobahn which use p1609.2.

The p1609.2 certificate structure is based on X.509, but with modifications to meet C-ITS specific needs (such as pseudo-anonymization). Such certificates have embedded "service specific permissions" (SSP) and can be issued based on the "role" of a vehicle.

The *C-ITS delegated act* was stopped in 2019, after several member states and stakeholders objected to a lack of technology neutrality, claiming that the act favored ITS-G5 technology. Today there are two main communication technologies for C-ITS; ITS-G5 based on Wi-Fi technology, and C-V2X which is currently not part of C-ITS standards, but work is ongoing to provide C-ITS standards over Internet. The first cybersecurity standard based on the C-ITS certificates is available as ISO 21177.

To achieve interoperability between the various C-ITS services in Europe, a common trust system and standard protocols are needed. Proper anonymization of data is also crucial. The European Commission (EC) has the role as central trust provider (CPOC and TLM).

There are three levels of ECTL certification: L0, L1 and L2. L0 is intended for pilots and testing and does not have strict security requirements. L1 and L2 are now ready for deployment, and the EC intends to go live from November 2024. The lack of L1 and L2 accreditation until now is likely one of the reasons why VW provides their own root CA which is currently not in the EU CCMS hierarchy.

Parallel PKIs is a complicated matter. The p1609.2 certificates have embedded, service specific permissions, so the certificates themselves are service specific. This means that there will generally be different root CAs for different services. There are some discussions (both national and trans-national) regarding "service groups" and how these should be handled in terms of certificates.

It is not easy to say which actors are natural root CA candidates for different services. The different providers in the trust list (ECTL) will also be service specific, and a C-ITS station (e.g. a car) can potentially have certificates from dozens of root CAs.

Regarding ongoing initiatives in Norway, the informant mentioned that the Norwegian NRA has an ongoing project to get a better overview of the PKI "status" in Europe and provide a roadmap/plan for future C-ITS activities. It is likely that the public sector in Norway will take the role as domestic trust anchor.

Norway is one of the countries opting for a hybrid communication technology, since it is not considered feasible to cover all C-ITS needs in Norway with short-range ITS-G5 alone. The expectation for Norway is a hybrid solution with ITS-G5 stations in certain locations (such as intersections with smart traffic lights) and relying on cellular technology elsewhere to prevent an unnecessary myriad of roadside stations.

The interviewee did not highlight specific challenges related to trans-national C-ITS services, and pointed out that there will likely be many C-ITS services in the future, where some will be international and others national or regional. There will likely be a wide range of "service types"

in the future, and handling the many service types may be just as challenging as handling trans-national challenges.

When discussing certificate revocation, two main approaches were mentioned for C-ITS. One is to perform revocation based on revocation lists which have to be managed and distributed, and the other is to have short-lived pseudonym certificates which expire frequently. The "break even" between these two options is essentially when the distribution of a revocation list requires the same amount of time as the lifetime of a short-lived certificate. According to the informant, a revocation approach has been chosen in the US, while European solutions rely on short-lived pseudonym certificates.

5.1.6 France

The responsibility of operating/offering the EU Root-CA service was put out to tender by the EU commission in April 2019[9], and in the process of selecting a provider, the French company Eviden (Atos) was chosen in December 2019[10]. Eviden is now responsible for the operation of the EU Root-CA, enrolment authority and authorisation authority.

Currently, more than 40 actors are connected to the EU Root-CA solution. The group of actors represent a wide range of European countries and sectors and comprises manufacturers who develops C-ITS stations and operators of C-ITS stations. According to the interviewees, actors from Germany, France, Italy, Netherlands and Austria are considered most active. During the interview the interviewees provided an overview of the largest station providers connected to the EU Root-CA (see Table 3), however, they could not share the full list with us, as they are only operating the EU Root-CA on behalf of the EC.

Table 3: Some station providers connected to the EU Root-CA

Station providers:
Hyundai
Fiat
Bosch
Qualcomm

In addition to the station providers listed in the table above, there is also quite an extensive list of Italian companies, mostly small R&D operators, connected to the EU Root-CA.

The level of maturity amongst the European countries varies greatly. Some countries have a strong PKI policy and are willing to invest and deploy national systems, whereas others are not that involved and prefer the market to decide what it will do. In Germany, Austria and France there is the will to deploy actively, and they have a proactive strategy.

[9] https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4701
[10] https://www.car-2-car.org/fileadmin/press/pdf/2020_06_18_EU_Root_CA_Webinar_Presentation.pdf

Maturity and coverage do not only depend on technical maturity of the solutions provided today, but there are also several elements that can interfere or accelerate the deployment of C-ITS. First, there is the regulation. Today there is no delegated act, so it is not compulsory to deploy C-ITS services, but when the delegated act enters into force, it will accelerate the deployment. Second, there is the Euro NCAP[11] test for cars, which is a common safety rating system for new cars in Europe. The score in this test has a high impact on the sales of cars. Five stars is the best score, and if a car receives perhaps only three stars it is a bad publicity for the brand and the sales will decrease. So, including C-ITS services and their interoperability as a part of the test will ensure that car manufacturers implement these services. A third point that was mentioned was that today there is only the Volkswagen group who has integrated and deployed C-ITS PKI. If another large car manufacturer, such as Stellantis or Renault also releases such solution, it could make others follow.

Administratively connecting to the EU Root solution at L0 is a simple and streamlined process. At L1, the procedure remains relatively uncomplicated, however, it does require verification of certain compliance factors. The technical integration of C-ITS stations is also regarded as straightforward. Among the 40 actors connected to the solution, only a few of them needed technical support.

Several factors can impact the decision to adopt the EU solution or opt for a private alternative. Primarily, the choice depends on the specific use case scenarios. For instance, France has decided to maintain sovereignty of their cryptography solution for the security of the C-ITS services delivered in the country. They have decided to invest in the PKI and maintain independence from decisions made at the European level. Another consideration is the need for a specific service that is incompatible with the use of the Central European PKI because it is a shared service, and they want to have some specific use cases only for themselves. If, for example, a city wants to give some specific permissions to busses so that they can request the traffic light to remain green to move forward and not having to stop they can do so at the central European PKI level, but then this applies to all busses. If you want to give that right exclusively to the busses of your city, and not to the city that is close by, then you need a private PKI to differentiate your messages or your certificates from those of other cities.

In the standard you have some technical aspects that are covered, but at the usage level you also need harmonisation, so this is what the car2car consortium and C-Roads platform are using. They are defining the harmonisation of some specific use cases[12]. Today we do not have enough harmonisation to provide common solutions for similar use cases. This is where you would have to opt for a private PKI.

The main challenge is not related to the PKI itself, but to the hardware deployment and installation on the roads. It is complex and has a high cost, which can make the public administration reluctant to accelerate their C-ITS deployment. For example, L2 PKI can only accept L2 stations on the PKI side. It is relatively easy to be audited and to maintain this level of security for many years. However, on the hardware side, you must be compliant with some

[11] https://www.euroncap.com/en

[12] https://www.c-roads.eu/platform/about/news/News/entry/show/c-roads-publishes-harmonised-c-its-specifications.html

protection profiles that are evolving, and the regulations will also be evolving. At some point, you might have stations that have been produced in 2024 that are not valid anymore in 2029.

The informants' further opinions are summarized around the following key points:

- **European C-ITS PKI deployment:** The informants discussed the current state of European C-ITS PKI deployment, mentioning that they have over 40 actors connected to their solution, including manufacturers and operators from various sectors and countries.
- **Challenges and solutions:** The discussion covered challenges organizations face when connecting to C-ITS solutions, such as technical integration and administrative processes. They highlighted the ease of onboarding for L0 on the European Root CA and the open criteria for companies to comply with regulations.
- **Technical support and standardisation:** The importance of technical support for actors and the role of standardisation bodies like ETSI in ensuring interoperability was emphasized. Plug tests were mentioned as a key activity for verifying standards implementation.
- **Private vs central European PKI:** Reasons for choosing private PKI solutions over the central European PKI were discussed, including sovereignty, specific use cases, and the critical mass justifying investment.
- **Hardware deployment and privacy concerns:** The conversation touched upon the complexities of hardware deployment and installation, the evolution of protection profiles, and the need for hardware to be compliant with changing regulations.
- **Future predictions and strategies:** The participants speculated on future requirements for C-ITS services, the potential need for hardware updates, and the impact of second-hand car markets on PKI management.
- **Closing remarks:** The interview concluded with acknowledgments of the usefulness of the discussion and a request to share the presentation and any other relevant materials.

Key take-aways:

- There is a growing network of actors connected to the European C-ITS PKI, indicating progress in deployment.
- Technical and administrative ease of integration is crucial for expanding C-ITS services.
- Private PKI solutions are chosen for reasons of national strategy, specific use cases, and when the scale justifies the investment.
- Future-proofing C-ITS services against evolving regulations and ensuring interoperability are ongoing challenges.
- The interview highlighted the dynamic nature of C-ITS PKI deployment and the various factors influencing decisions at the national and organizational levels.

5.1.7 Summary of key inputs

In the following, a selection of key topics and challenges from interview discussions are summarized.

Trust hierarchy, roles and accreditation

The informants were reasonably acquainted with the EU CCMS trust model, but most were uncertain about how roles and responsibilities should be distributed between the various stakeholders. The trust hierarchy “picture” is expected to get clearer as C-ITS services become more widely adopted and more mature.

There is a general lack of PKI expertise and resources in the C-ITS community, and many of the needed PKI services are expected to be outsourced to private companies.

For a trust provider (root CA) to be included in the ECTL, it has to be audited and approved by an independent party according to the accreditation scheme defined by EU CCMS (Joint Research Centre, 2024). There are three different security levels for accreditation: L0, L1 and L2. L1 and L2 have recently become ready for deployment (EU CCMS policy documents were finalized in June 2024), so we should expect to see L1 and L2 certifications in the near future.

Trans-national compatibility

Based on workshop and interview discussions, we expect a C-ITS ecosystem with multiple services and multiple PKIs, where some need to operate across borders while others don't. Any C-ITS functionality related to traffic safety should be managed such that messages can flow easily between the involved vehicles and roadside stations, regardless of which country a given vehicle or roadside station "belongs" to. In addition to safety related services, C-ITS services which involve for example customs information or payment solutions may also require trans-national cooperation and harmonization. Most existing C-ITS services currently operate within rather than across country borders, so there is very limited operational experience regarding how to manage cross-border challenges.

Communication technology

There are two main types of communication technology which enable C-ITS services, each with their pros and cons.

- ITS-G5: Short range communication based on Wi-Fi technology. Mainly uses the IEEE p1609.2 certificate standard. ITS-G5 is a well-defined and open standard which can be applied by any provider with relative ease and high compatibility with other ITS-G5 solutions. This technology allows for very fast (but local) communication and is well suited for time-critical services involving fast-moving vehicles, such as smart traffic lights.
- C-V2X: Long range communication based on cellular technology such as LTE and 5G. C-V2X also enables vehicles and other C-ITS stations to communicate directly with each other. At present, C-V2X is not included in the C-ITS standards, but work is ongoing to provide C-ITS standards over the Internet. Since it involves several different cellular technologies, C-V2X is less standardized and involves proprietary protocols, but the certificates used generally follow the X.509 standard. C-V2X is significantly slower than ITS-G5, but greatly reduces the need for roadside C-ITS stations since it relies on mature infrastructures which already have good coverage in large parts of the EU.

The C-ITS delegated act, which was proposed by the European commission and aimed to set a legal framework for the use of C-ITS in the EU, was stopped in 2019 due to objections from several member states and stakeholders. The opponents claimed that the principle of technology neutrality was violated because the proposed act favoured ITS-G5 and included requirements which would effectively exclude C-V2X from C-ITS applications. The idea of a "hybrid communication" approach, where ITS-G5 and cellular technology can complement each other, has since gained momentum, as evidenced by initiatives such as the C-Roads hybrid communication task force[13].

There is an ongoing competition between ITS-G5 and C-V2X among car manufacturers, as some have chosen ITS-G5 for their vehicles, while others have opted for C-V2X. This competition is hampering C-ITS implementation, since stakeholders are reluctant to invest in technologies and solutions with such uncertain prospects.

Several informants and workshop participants claim that there is still too much focus on short-range ITS-G5 communication and would like to see more guidance for how to implement C-ITS services with C-V2X communication.

Past (and ongoing) discussions regarding long-range vs short-range communication have been complex and involved a wide range of political, economic and technological considerations. Based on the interviews and workshops, it seems that most member states are now opting for a hybrid approach.

Cost

There are various types of costs to consider for providers of C-ITS services and their PKIs, which can influence the plans and strategies of NRAs and other stakeholders. In the interviews and workshops, a few types of cost considerations were mentioned which we would like to highlight:

- Cost expectations as incentive to delay C-ITS adoption: Since C-ITS involves relatively new technologies which are rapidly evolving, several stakeholders will be tempted to "sit on the fence" and let other actors (the early adopters) bear the costs while the technology matures and becomes cheaper. The fear of "not keeping up" with technological advancements seems quite insignificant.
- Cost related to obsolete hardware: Since C-ITS capabilities are integrated in vehicles which may have a lifetime of up to several decades, there are some concerns that the C-ITS infrastructure will evolve "too fast" compared to the lifespan and future proofing of today's vehicles (and other C-ITS hardware currently in operation). Such obsolescence concerns are much less common when it comes to e.g. general IT hardware which has a much shorter lifespan. If C-ITS hardware becomes obsolete prematurely, it will either trigger replacement/upgrade costs, or lead to a reduction in available services for the outdated devices.
- Cost of PKI operation: Interview informants and workshop participants seem generally more concerned with operational costs (OPEX) than initial investments (CAPEX), as the former is much harder to get approved in the respective organizations. As mentioned in sections 5.3.7 and 5.3.9, the cost of support services

[13] https://www.c-roads.eu/platform/activities/tf-hybrid-communication.html

is one of the biggest operational costs, and we don't expect the cost picture for C-ITS PKI operation to be much different.

User adoption

Most new technologies (including C-ITS) depend on significant user adoption to become successful. Unless providers see good opportunities for commercialization and profit, they will be reluctant to make the necessary investments. On the other hand, end users are much more willing to embrace a product or service if it is already well-functioning and mature. This "chicken-and-egg" challenge is highly relevant for C-ITS as well.

For private individuals who purchase modern cars, the C-ITS services will generally be perceived as a property or functionality of the car itself, and the user's experience with the C-ITS functionalities will directly influence customer satisfaction and reputation for car manufacturers. For this reason, car manufacturers are expected to have strict requirements for the C-ITS services which they choose to integrate in their cars.

5.2 Expert workshops

This section presents the results of the expert workshops held in the project. Initially, the expert workshop was planned as an in-person event at the TRA conference in April 2024. However, it was decided to replace it with two online events to allow more people to join and avoid the risk of not being able to recruit enough experts at the TRA conference. In total 26 informants participated in the workshops, and 13 of them joined our breakout sessions. The results from these workshops have been combined and are presented in the following paragraphs.

(Joint Research Centre, 2023, 2024)The European Commission aims to offer support for European C-ITS deployment with three different levels of trust list management (TLM) services. The first level, L0, is used for testing and pilot purposes. L1 is the intermediate level, and here, stations and use cases are in operation, but with some exceptions regarding regulations. The final level is L2, and here the stations and use cases need to be fully compliant with the regulation. L0 only requires a self-declaration, whereas L1 and L2 entail a regulation assurance process.

When implementing a C-ITS PKI solution, there are three different approaches to take. The first approach is for the organization to take care of all the tasks and responsibilities themselves. The second option is contracting each part of the system, and the third option is to buy everything as a package.

There are multiple use cases for C-ITS PKI, and the service is offered by several providers, although none are currently operating at large scale. Workshop participants mentioned that it is important to identify the providers of the Root CAs. TeskaLabs[14] was mentioned as one of the providers, and it was also mentioned that car brands explore the opportunities of offering their own PKI. Volkswagen (VW) is one of the car brands offering their own PKI, which is currently being used in Austria and Italy. The VW PKI is operational and at the L1 stage. Other

[14] https://teskalabs.com/

Root CA providers mentioned were Microsec, Saesol[15], Autocrypt[16] and Greenhills[17]. One of the informants said that in Europe we should only focus on the providers of the Root CAs because the EC takes care of the PKI CCMS management and governance.

The EU Root CA has more than 40 registered actors on L0. The solution is free of charge, and this will also be the case for L1 and L2. One of the informants, who had experience with both the EU Root CA and the solution from a different provider, mentioned that connecting with the EU Root CA had been more challenging than connecting with the other provider. They faced several challenges during the implementation phase, including in the administrative process. However, the informant was not familiar with the entire situation and could not provide more details on this matter.

The timeframe for setting up the solution and having something that works depends on several factors. First, the procurement and tendering process takes time. You need to decide if you want to do it yourself or if you want to contract it to others. Further, you need time for the enrollment of the stations. There are many intermediate steps, and it is difficult to set an upper time limit. One of the informants reported that it took longer than expected.

The informants briefly discussed the costs associated with C-ITS PKI. They mentioned that these costs play a role and that from an NRA perspective, justifying the operating expenses is more challenging than advocating for the initial setup costs of the solution.

5.3 Lessons learned from PKI operations in other sectors

The lessons learned from operating Public Key Infrastructure (PKI) can be drawn from a wide range of sectors. These include, but are not limited to general information technology, healthcare, finance, government, telecommunications, manufacturing, education, maritime and aviation. Selected publications that provide relevant challenges and advice on these are summarised below.

5.3.1 Information Technology (IT)

The IT community is well-known for using PKI for services such as secure email, trust in websites, identification of users, establish session keys for secure communications, and software verification through code signing. Notably, web browsers come pre-installed with X509 root CA certificates issued by a number of trusted Certificate Authorities (CAs). This collection of self-signed certificates serves as the root of trust. When a browser connects to a secure website, the server sends its SSL/TLS certificate to the browser. The browser checks if the certificate was issued by one of the trusted CAs. This is done by comparing the signature on the TLS certificate with the public key of the CA. Although the browser does not need to contact the CA to validate the signature, it does need to contact the CA to verify that the certificate hasn't been revoked. This is typically done using base and delta Certificate Revocation Lists (CRLs), the Online Certificate Status Protocol (OCSP), or OCSP Stapling.

[15] https://www.saesol.tech/
[16] https://autocrypt.io/
[17] https://www.ghs.com/

A diverse range of security companies and non-profit organisations operate as CAs, such as Comodo, Let's Encrypt (free), DigiCert, GoDaddy and Globalsign (McKinnon, 2022). Many of these operate in industry specific sectors as well.

When it comes to lessons learned on operating PKIs in this environment, there are some dated publications on this matter ((Ellison & Schneier, 2000; Guida et al., 2004; Gutmann, 2002)), emphasizing:

- A general problem with PKIs is the hierarchical structures, while in the real world there may be non-hierarchical organisations. Therefore, the recommendation is to design the PKI according to the real world, rather than constraining the real world to match the PKI.
- Certificates and PKIs specifically designed to address a particular problem are much easier to work with than a one size-(mis)fits-all PKI design.
- Identities should be locally meaningful and globally unique.
- There are several challenges related to CRLs, including how frequent these should be published (distribution is expensive, checking is time-consuming and subject to denial-of-service attacks). The recommendation here is simply to design the PKI so that it does not require certificate revocation, thus avoiding many of the problems.
- Users need to know how their environment will change when introducing a PKI.
- Try to estimate how many uses will need support services.
- Design processes that allow identity credential changes, this is bound to happen.
- Avoid language barriers, do not restrict to English as the information management language.

In addition to the above, general PKI advice can be provided by national cyber security bodies, such as NCSC[18].

5.3.2 Healthcare

PKI is used in the healthcare sector for many different purposes, including, but not limited to secure access to electronic medical records and ensuring the integrity of transmitted medical data. A study (Mantas et al., 2012) looking at the open issues of PKI security in large-scale healthcare networks identifies the choice of trust model as the main issue for inter-organisational PKIs. Furthermore, the complexity of certificate path processing is another critical factor that affects the efficient adoption of PKI technology. A recommendation from the authors is that end-entities should be provided with information about the CA liabilities and the quality-of-service parameters of the issued certificates. They also recommend the use of trust lists to determine whether end-users making request for healthcare services should be considered.

5.3.3 Finance

Financial institutions use PKI related to for example secure online banking, cardholder authentication, and secure email. The international standard *ISO 21188:2018 - Public key infrastructure for financial services — Practices and policy framework* (ISO, 2018) sets out a framework of requirements to manage a PKI through certificate policies and certification

[18] https://www.ncsc.gov.uk/collection/in-house-public-key-infrastructure/pki-principles

practice statements and to enable the use of public key certificates in the financial services industry. The recommendations from this standard are:

- A PKI should be managed through certificate policies and certification practice statements. These are essential for defining the different levels of trust within a PKI and for detailing the procedures that a Certification Authority (CA) will employ in issuing and managing certificates.
- To manage risks, the standard states that control objectives and supporting procedures should be defined.
- Operational practices relevant to the financial services industry and their information systems should also be defined. These practices are important for ensuring the effective operation and management of the PKI.
- To ensure flexibility and scalability of the PKI, the PKI should support practices that allow for multiple certificate policies.

The standard also draws a distinction between PKI systems used in closed, open, and contractual environments. This implies that the implementation and operation of PKI may vary depending on the specific environment, which can pose challenges.

5.3.4 E-government

PKI is used in e-government solutions, including secure email, virtual private networks, and digital signatures for e-services. The paper titled “A good-practice guidance on the use of PKI services in the public sector of the European Union member states” (Gritzalis, 2005) provides several lessons learned from operating a PKI in the government sector. However, the current situation described in the paper is very much dated (2005), so it is difficult to assess the relevance of these recommendations today. The main challenges mentioned here were flexibility, scalability and interoperability.

More recently, the *electronic IDentification and trust Services* (eIDAS) (EU, 2024a) regulation has set out to facilitates secure cross-border transactions for the EU internal market by establishing a framework for digital identity and authentication. It came into effect between 2016 and 2018 and has enabled electronic signatures, digital certificates for natural persons and Websites, electronic seals and trusted timestamps. In 2021, the European Commission proposed new qualified trust services for electronic archiving, electronic ledgers and the management of remote signatures and seals. A comprehensive set of guidelines, which include technical requirements, formats of trusted lists and procedures, have been instrumental in harmonization and interoperability across the national electronic ID systems across Europe. Still, there were shortcomings identified from a consultation with various stakeholders, which has led to a new proposed regulation on *European Digital Identity* (EUDI) (EU, 2024b). Large-scale pilots are going to test the technical specifications and software prototypes for the European Digital Identity Wallets.

5.3.5 Telecommunications

Telecom companies use PKIs for secure administration of distributed networks, secure VPNs, and protection of infrastructure.

A study from 2021 (Hadan et al., 2021) from the telecom domain describes a gap between security and policy experts' perceptions of PKI failures and real-world PKI incidents between 2001-2020. The study found that experts identified weak cryptography and software bugs as the major and well-known sources of error. In reality, the primary cause of certificate failures is CAs' misinterpretation of baseline requirement, meaning the policies and processes used to determine which CAs should be trusted. This suggests that understanding of PKI operation and its challenges needs to be grounded in practical, real-world experiences, not just theoretical knowledge. The same study also found that systematic weaknesses in organisational practices can create risks for all who rely upon PKIs. On a positive note, the study identified organisational and configuration choices that could avoid or mitigate some of the risks associated with PKIs. This suggests that proactive planning and strategic decision-making can enhance the effectiveness of a PKI.

A survey paper (Ramadan et al., 2016) on PKI for mobile communication systems describes latest proposed works on the security of GSM, CDMA, and LTE cellular systems. It presents the security issues for each generation of mobile communication systems, studies and analyses the latest proposed schemes, and gives some comparisons. Though the paper concludes that public key cryptographic approaches are good from a security point-of-view, they are also computationally extensive and have more signalling overhead compared to symmetric key encryption. A solution to this could be to use efficient lightweight schemes such as *identity-based cryptography* (IBC) and *certificateless-public key cryptography* (CL-PKC). These do not require a CA, and this leads to lowering the processing time (delay) and handshaking processes.

5.3.6 Education

Educational institutions use PKI for secure access to digital resources, secure email communication, and identity management. A publication (Linden et al., 2002) with pilots from Finnish institutions focus on the applicability of PKI and smartcards. The authors come to the conclusion that it is really the user administration of the institute that needs focus in order to modify existing services and implement new ones. A too technology-oriented view to the problem should be avoided.

Another paper (Hermann, 2001) recommends to facilitate interoperability between organisations through so-called bridge-CAs. A bridge CA determines the policy mapping between the bridge's participants.

5.3.7 Maritime

The paper "PKI vs. Blockchain when Securing Maritime Operations" (Rødseth et al., 2018) compares the two technologies, indicates strengths and weaknesses of each, and gives some examples of typical applications where each of the technologies can be used. These applications include updates of nautical safety information to the ship, port state reporting from ship to shore, and approval letter for ship building process. One key challenge at sea is finding a neutral root CA that different flag states can accept. Furthermore, connectivity could be an issue as ships could be on open seas for days or weeks. This limits the capabilities of renewing certificates or revoking certificates. All CA certificates should be downloaded and stored locally before setting sails (Frøystad, Bernsmed, & Meland, 2017).

The Norwegian project CySIMS-SE conducted a study (Frøystad, Bernsmed, Meland, et al., 2017) which included the PKI implementation process and costs for the Norwegian Maritime Authority. A premise here was that international shipping is dependent on maintaining a reasonable and normally relatively low cost on its business operations and this imposes limitations on which PKI solutions could be acceptable to the industry. The project also analysed the pros and cons of outsourcing of the PKI service versus inhouse ownership and management. The cost of implementing PKI obviously varies with each installation, but there are some common expenses that occur, such as planning and assessment, facilities, hardware and software, installation and configuration, disaster recovery, backups, root key generation, audits, and maintenance and operations. The price per user decreases as the number of certificates increases, but it is really the personnel cost that is the main driver. In that sense, it does not matter so much whether you are managing 10 000 or 50 000 entities, having staff available 24/7 is a much harder requirement. Having such support services can overshadow most of the other costs, as these can often be automated.

5.3.8 Aviation

The aviation sector has many commonalities with maritime, as connectivity can be limited and with international operations. As presented by Patterson (Patterson, n.d.) in an *International Civil Aviation Organization* (ICAO) information paper, PKIs are being used in various aspects of air transport, including Secure ACARS, Gatelink, Field Loadable Software, Electronic 8130 Airworthiness, Electronic Flight Bag, Signed Flight Plans, Manifests, weather reports, maps, etc. A major challenge is that setting up a CA is expensive, and unless there is convergence on a single policy, there will be no providers willing to set up those CAs. Moreover, key management is still a work in progress. According to Patterson, it is important for there to be only one PKI standard for the industry. A cross-certified environment makes it less expensive to set up a CA.

Bernsmed et al. (Bernsmed et al., 2017) provide a set of recommended security requirements for datalinks enabling future air traffic management services. These are derived from the needs of future ATM services and can be a useful source for defining similar requirements in C-ITS, e.g. related to integrity protection, data-origin authentication and overhead of cryptographic protection. At the same time, the authors emphasize the results from a security analysis may have a very short lifetime as *"threats that are relevant today may be irrelevant tomorrow and new threats that cannot be foreseen may appear in the future"*.

Relevant standards that come from the aviation industry include ARINC 842-1 (ARINC, 2018) on life-cycle management of asymmetric keys that are used to secure interactions among systems. This standard complements ATA Spec 42 (ATA, 2020), which specifies a digital identity management framework and standard digital certificate profiles recommended for use across the air transport industry. ARINC 835-1 (ARINC, 2014) provides guidance for security of loadable software parts using digital signatures.

5.3.9 General challenges and lessons learned

Looking across sectors, we can see that there are many of the same issues that emerge. Especially the choice of trust model is a commonality when dealing with inter-organisational PKIs. Furthermore, operational practices should be designed to reflect existing organisational structures, as these are more difficult to change. Focusing on mostly technology, and not

sufficiently on the organisational aspects, can easily lead to an expensive and unsuitable PKI design.

Another general advice is to keep the complexity as low as possible. For instance, cross-certified environments are difficult and expensive to manage. Avoiding CRLs is another approach to reducing complexity, though this might make the system more vulnerable in case of key compromises. Support services is seen as a major cost driver in several sectors.

There are some sector specific challenges, such as limited connectivity or low bandwidth, that require special considerations related to e.g. cryptographic overhead. However, this is less of a challenge for C-ITS which can benefit from terrestrial communication infrastructures.

We have also seen some PKI advice that are collected from several sectors. A survey (Ponemon, 2020) conducted by the Ponemon Institute in 2020 with responses from 603 IT and security professionals revealed some of the fundamental problems in PKI management:

- There are often insufficient skills and resources to operate a PKI. Only 38% of respondents stated that their organisations have enough IT security staff members dedicated to their PKI deployment.
- There is a lack of investments in modern PKI infrastructures. Manual and outdated methods are used to deploy and manage PKIs.
- Emerging connected devices (e.g. IoT devices) present a significant challenge for enterprises. Attackers seek to exploit weak credentials to steal data, disrupt services or distribute malware.
- Failed audits due to insufficient key management practices and compromised or rogue certificate authorities (CA) are the most frequent and most serious problems faced by organisations when it comes to managing PKI and cryptography.
- Less than half of respondents (44%) are confident in the security of their root CA.

Additional PKI pitfalls mentioned by the PKI provider Sectigo (Callan, 2021) include the use of too weak keys, unnecessarily long certificate lifespans, improper protection of private keys, lack of policy consistency.

In order to address these problems, the respondents from the Ponemon survey prioritised the following four strategic priorities for their enterprises:

- Authenticating and controlling IoT devices.
- Knowing the expiration date of certificates.
- Reducing complexity in their IT infrastructure.
- Reducing the risk of unknown certificates in the workplace.

The first three of these should be just as relevant for C-ITS.

6 D2.1 Conclusions

6.1 Overview of PKI roll-out

The current status for PKIs for European C-ITS services is that most countries have a very limited rollout. Although many countries' NRAs have conducted pilots and testing of new concepts, only a few (most notably Germany and Austria) have established a significant C-ITS road infrastructure. There is general consensus that the respective NRAs will have an important role regarding the establishment and operation of PKIs for public C-ITS services, but the PKI service itself will likely be outsourced to specialist companies in many cases. Although there seems to be a wide selection of private companies who can provide PKI services, it is important to ensure that C-ITS specific needs are properly identified and met. PKI expertise and resources are scarce among many C-ITS stakeholders, so there will be a need for guidance when establishing and applying best practices.

The C-ITS services which are currently available are mainly public services related to traffic safety and road work information, but many other C-ITS services are expected to be offered in the future. As the number of C-ITS services increase, so will the number of PKIs. The various PKIs will need proper accreditation in order to be included in the ECTL, such that they can operate within the EU CCMS trust hierarchy.

It is expected that providers of C-ITS services (including NRAs) will have to cooperate closely with car manufacturers in order to get their C-ITS services "approved", since the performance of integrated C-ITS functions will directly influence the user experience and the car manufacturer's reputation. Manufacturers are therefore likely to demand high performance and reliability in the C-ITS services which they integrate in the vehicles.

6.2 Multiple PKIs

Even though C-ITS is at an "early stage" and the informants predict a strong increase in the number of services, there are already a significant number of providers that offer C-ITS PKI services. 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 Volkswagen, who have decided to establish and operate their own PKI.

Operating a PKI requires specific competence and resources, and many C-ITS stakeholders therefore choose to focus on core business and outsource their PKI needs. According to most of the informants (mainly representatives from NRAs) their organizations did not have the necessary competence and capacity to operate their own PKI.

Several providers of C-ITS PKIs have been identified in the interviews and workshops; these are listed in Table 4.

Table 4: Overview of identified C-ITS PKI providers

PKI provider
Eviden/Atos (EU Root CA)
Microsec

Telefonica (This PKI is operated by Criptographic Services - Cybersecurity Deparment under Telefonica Digital Security Unit using 5G Telefonica network capabilities)
Swarco[19]
TeskaLabs[20]
Autocrypt[21]
IP Telecom, Serviços de Telecomunicações S.A.
CTAG
ETAS GmbH / ESCRYPT GmbH
Integrity Security Services LLC[22]
Volkswagen AG[23]
BOSCH
Saesol
Greenhills

6.3 Lessons from other sectors

One general lesson from other industries is that operational practices need to reflect organizational structures. Too much technology focus can often lead to an expensive and unsuitable PKI design. In that respect, 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.

Another general piece of advice from other sectors is to minimize complexity, for example by avoiding CRLs. Various C-ITS services are already avoiding CRLs (with the use of short-lived pseudonym certificates), but the main motivation for this seems to be response time (and privacy considerations).

Limited PKI expertise and resources is a challenge in various sectors, and as discussed in 6.1, this is the case for C-ITS as well.

[19] https://www.swarco.com/solutions/connected-driving/c-its-ready-hardware
[20] https://teskalabs.com/solutions/seacat-cits-security
[21] https://autocrypt.io/products/pki/
[22] https://www.ghsiss.com/wp-content/uploads/2023/03/ISS_Root_CA_Certificate_Policy_v1_4.pdf

[23] https://certdist.volkswagen.de/faces/components/viewCert_CP.xhtml

Limited connectivity and low bandwidth are significant challenges in certain other sectors, but for C-ITS these will be mostly avoided by the use of terrestrial communication infrastructures. There are, however, particularly high connectivity demands for certain C-ITS services, as they need to reliably and efficiently transmit safety-critical (and time-critical) information, often in challenging circumstances such as high traffic density and poor weather conditions. Despite the robust terrestrial infrastructure, there may therefore still be significant connectivity challenges to manage.

Lastly, in addition to the lessons discussed above, we can repeat some of the generic challenges mentioned in 5.3.9, which were identified by the Ponemon survey (Ponemon, 2020):

- There is a lack of investments in modern PKI infrastructures. Manual and outdated methods are used to deploy and manage PKIs.
- Emerging connected devices (e.g. IoT devices) present a significant challenge for enterprises. Attackers seek to exploit weak credentials to steal data, disrupt services or distribute malware.
- Failed audits due to insufficient key management practices and compromised or rogue certificate authorities (CA) are the most frequent and most serious problems faced by organisations when it comes to managing PKI and cryptography.
- Less than half of respondents (44%) are confident in the security of their root CA.

7 D2.2 Findings and guidance

This chapter presents findings and guidance based on the work done in the second part/phase of the project. In addition to being based on deliverable D2.1, the D2.2 work also involved 2 additional workshops and one additional interview, as well as internal meetings and more literature review. The following sections present a selection of topics and challenges which have been identified as particularly important in this project, along with guidance/suggestions for how NRAs may approach them.

7.1 Main challenges and generic recommendations

This section presents a set of possible approaches to addressing the main challenges identified in D2.1. These suggestions are intended to serve as general guidance and should not be seen as definitive solutions. Given the wide variety of use cases and stakeholder contexts, the relevance and applicability of each suggestion will naturally vary. The list is not exhaustive, nor are the approaches presented necessarily the most effective in every situation. Rather, they are intended to support further exploration and adaptation to specific needs and circumstances.

Table 5 presents the challenges related to C-ITS PKI implementation and operation which were identified in deliverable 2.1 (“Operation of Public Key Infrastructures: State-of-the-art and best practices”) along with some general mitigation strategies. These recommendations will be discussed in more detail in chapter 8.

Table 5: Challenges related to C-ITS PKI implementation and operation from Deliverable 2.1.

Challenges	Recommendations
PKI implementation challenges: Complex and challenging to implement and manage PKI systems, in particular in terms of regulatory and operational requirements. Managing a PKI system requires strict processes and significant expertise, which are often challenging to maintain consistently over time.	- Hire skilled resources - Conduct regular audits - Establish a community/forum for NRA representatives with PKI responsibilities, conduct training, workshops, etc.
Technological challenges: Concerns regarding the impact of patents and proprietary technologies on the accessibility and cost of communication technologies, particularly how these might affect the broader deployment of C-ITS technologies.	- Open standards among stakeholders should be promoted at an EU level in order to reduce dependency on proprietary technologies and patents
Workforce and expertise: Difficult finding the right resources to manage a PKI system. The niche nature of the expertise, not commonly taught in traditional educational settings.	- Leverage managed PKI services to outsource PKI management, reducing the burden on internal teams and ensuring access to experts
Value chain: High costs and unclear financial responsibilities. The allocation of costs across	- Enhance supplier collaboration, utilize technology and automation.

Challenges	Recommendations
stakeholders lacks clarity, with unresolved questions about who benefits from services and who bears the financial burden.	- Establish/participate in interest groups for C-ITS service providers
Interoperability: Ensuring seamless communication across different systems and brands	- Adhere to the EU standard for C-ITS PKI
Cross-border information exchange: Managing transitions between different PKIs when vehicles cross borders.	- Use the EU C-ITS PKI to allow for effective data exchange across borders
Security: Balancing the need for service availability/robustness with requirements for data integrity.	- Conduct regular security audits - Apply adequate monitoring of PKI infrastructure to detect technical and security issues
Political barriers: Conflicting priorities between stakeholders (and between countries) make it difficult to align efforts for C-ITS implementation.	- Foster collaboration among stakeholders, develop innovative policies, and address legal and institutional barriers through strategic planning
Hardware deployment and installation on the roads: complex and has a high cost, which can make the public administration reluctant to accelerate their C-ITS deployment. Protection profiles are evolving and there is a fear of e.g. having stations produced in 2024 not being valid anymore in 2029.	- Encourage collaboration between public administrations and private companies to share costs and expertise. - Invest in scalable and flexible infrastructure solutions that can adapt to future changes
Future-proofing C-ITS services against evolving regulations and ensuring interoperability are ongoing challenges.	- Adopt scalable and flexible infrastructure solutions, embrace emerging technologies, and prioritize modular architecture - Ensure backwards-compatibility when feasible
User adoption: Most new technologies, including C-ITS, depend on significant user adoption to become successful. Unless providers see good opportunities for commercialization and profit, they will be reluctant to make the necessary investments. On the other hand, end users are much more willing to embrace a product or service if it is already well-functioning and mature. Car manufacturers are expected to have strict requirements for the C-ITS services which they choose to integrate in their cars.	- Focus on developing mature, well-functioning products, provide clear commercialization opportunities, and engage with end users to understand their needs - Good collaboration between different C-ITS service providers

7.2 Communication technologies and certificate types

This section describes the main communication technologies for C-ITS in more detail, based on interview feedback and discussions from Deliverable 2.1 (see sections 5.1.5 and 5.1.7).

The two main categories of C-ITS communication in Europe are commonly referred to as *C-V2X* and *DSRC* (Dedicated Short-Range Communication). These main categories include both short-range direct communication and IP-based communication with backend servers. A simplified overview of these is shown in Figure 7, which we have compiled based on findings from interviews and workshops with informants. These communication technologies enable radiocommunication between different C-ITS stations, such as vehicles and roadside units (RSU). Depending on the type of message/transmission, both IP-based and non-IP-based communication is used. For safety messages requiring low-latency communication, a form of direct communication on the 5,9 GHz ITS band is used. Although C-V2X and DSRC both use the same frequency band for their direct short-range communication, they do so with different technologies (3GPP and IEEE 802.11p, respectively). For IP-based communication (e.g. with backend systems), C-V2X uses a cellular interface, while DSRC stations have to rely on roadside units to relay transmissions.

Short range communication (either DSRC or the PC5 part of C-V2X) enables fast and reliable local communication for safety messages. However, due to the limited range, a relatively high density of roadside units is necessary to provide good coverage for such safety communication. For many road operators, there will be a need for short range infrastructure in areas with high traffic density (e.g. urban areas), while other areas can be sufficiently covered by cellular technology (which greatly reduces cost as the communication can rely on existing infrastructure). Such a mix of C-ITS communication technologies is generally referred to as *hybrid communication*. The detailed specifications may vary, but in many contexts, "hybrid communication" has the same meaning as C-V2X. In some cases, the term may also include DSRC (either in addition to, or instead of PC5).

The various C-ITS services are typically divided into a few main categories:

- **V2V** (Vehicle-to-vehicle): Direct communication between vehicles to share information about speed, position and hazards, to enhance traffic safety and efficiency.
- **V2I** (Vehicle-to-infrastructure): Communication between vehicles and roadside infrastructure (e.g. traffic lights or signs) to optimize traffic flow and improve safety.
- **V2P** (Vehicle-to-pedestrian): Interaction between vehicles and pedestrians via mobile devices or sensors to prevent collisions and enhance pedestrian safety.
- **V2N** (Vehicle-to-network): Connectivity between vehicles and cloud-based networks for real-time traffic updates, remote diagnostics, infotainment, etc.

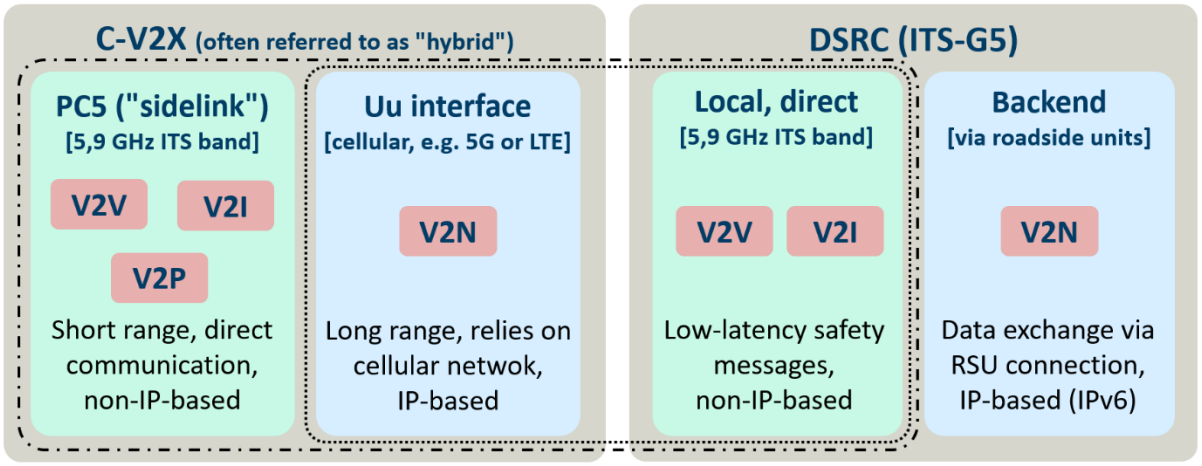

Figure 7: Overview of communication types and their interfaces and use cases. Green background denotes short-range and low-latency communication for safety messages, and blue denotes IP-based communication with backend systems. The dashed boxes show alternative definitions of "hybrid communication".

Some C-ITS services have unique safety related requirements (e.g. fast response without having to communicate with backend servers), which are not easily met with traditional X.509 certificates. To address these needs, the IEEE 1609.2 security standard was developed as part of the IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE). It defines a lightweight and privacy-preserving certificate format tailored for the high-speed, low-latency, and safety-critical environment of C-ITS.

As shown in Figure 7, there are various types of C-ITS services, where some involve IP-based communication with backend systems while others rely on short range direct communication on the 5,9 GHz ITS band. For IP-based communication and services (both within C-ITS and elsewhere), security is generally provided with TLS (Transport Layer Security), using X.509 certificates to authenticate parties and establish trust. For the short-range safety communication, however, TLS is not feasible because the necessary handshakes require both internet connectivity and time (where the latter is a scarce resource for time-critical safety communication involving fast-moving vehicles). Furthermore, TLS is designed for unicast (1-to-1) connections, while the short-range safety communication relies on broadcasting.

To meet the case specific challenges for C-ITS safety messages, a different set of security mechanisms has been defined in the IEEE 1609.2 standard, which specifies IEEE 1609.2 certificates and is optimized for low-latency and high-mobility environments. This standard offers lightweight authentication with low latency and offline operation. The use of encryption to protect the confidentiality of messages is optional, but the certificates are short-lived and pseudo-anonymous to ensure privacy. The IEEE 1609.2 certificates have embedded service specific permissions, which define what actions or services the holder of the certificate is authorized to perform. This enables the certificate issuer to define specific user groups (e.g. emergency vehicles) with different permissions.

The use of IEEE 1609.2 certificates (as demanded by the ITS-G5 standard) requires a specific PKI structure with a hierarchy of certificate authorities. For European C-ITS deployments, this

PKI structure and the corresponding trust hierarchy is defined by the EU CCMS[24]. The security architecture defined by EU CCMS shall ensure that all communications within the EU C-ITS ecosystem are secure, and that trust is properly established (especially for messages including safety-critical information). The certificates used within this architecture must follow the Certificate Policy document, which requires the certificates to be in accordance with ETSI TS 103 097 which is based on the IEEE 1609.2 standard. The IEEE 1609.2 certificates include information about service-specific permissions, and we expect different PKIs for different C-ITS services, resulting in a significant number of PKIs.

Although C-V2X PC5 communication currently does not comply with the ITS-G5 standard, the *messages* which are sent with PC5 can be signed with IEEE 1609.2 certificates. Among the interview- and workshop participants it is generally believed that it should be possible to have the same PKI structure for C-V2X PC5 communication as for ITS-G5 communication, such that the PKIs for short-range C-ITS services can be certified and utilized regardless of the underlying communication technology.

Based on feedback from interviews and workshops, getting ECTL certification for the PKIs which provide security for IP-based C-ITS communication is a big challenge. While it is technically possible to secure the IP-based transmissions with IEEE 1609.2 certificates, this is regarded by various stakeholders as unnecessary (since they are already secured with TLS), and this reduces the motivation for ITS-G5 compliance and ECTL certification.

Role-based and identity-based PKI systems

The safety messages which are transmitted via the 5,9 GHz ITS band are generally non-IP based and designed to be independent of infrastructure and internet connectivity. The IEEE 1609.2 certificates which are used to secure this communication do not contain information about the identity of the user (they are pseudo-anonymous), but they do contain service-specific permissions (SSP) based on the user's "role". The certificates (and the PKIs that manage them) can therefore be regarded as *role-based*. SSPs can for instance be used to enable only emergency vehicles to sign emergency vehicle warnings, and public transport priority to be restricted only to the respective stations[25].

Permissions issued in pseudonym certificates (Authorization Tickets or ATs) by an Authorization Authority (AA) must align with the permissions of their Root CA. The valid SSPs are inherited from the Root CA in a top-down manner, starting with the registration of the Root CA in the European trust model. Root CA setups can vary, including a single PKI branch for all SSPs, separate PKI branches for different SSP subsets, or mixed setups combining elements of both approaches[26].

[24] Updated versions of the EU CCMS policy documents can be found at https://cpoc.jrc.ec.europa.eu/Documentation.html
[25] C-ITS Security & Governance. C-Roads platform, Working Group 2, Task Force 1. Version 2.2.0, 28.05.2024
[26] C-ITS Security & Governance. C-Roads platform, Working Group 2, Task Force 1. Version 2.2.0, 28.05.2024

IEEE 1609.2 does not allow an AT to contain multiple SSP values for a given application service (each application service is specified with a *Provider Service Identifier*, or PSID), necessitating separate certificates for different Service provider IDs[27].

The PKIs which manage X.509 certificates, on the other hand, can be regarded as *identity-based*, as the certificates which are used to set up end-to-end connections contain identity information. For such sessions, trust needs to be established via a trusted CA which can authenticate identities. Assigning roles in such a structure requires a database which connects the role to the user, as the role is not included in the certificate.

7.3 Implications for NRAs implementing C-ITS communications

Based on input from the workshops and interviews, our impression is that the outlook for a harmonized coexistence of ITS-G5 and C-V2X-based services within a common PKI framework is cautiously optimistic, provided that the interoperability challenges are solved. The EU CCMS is designed to be technology-neutral, focusing on certificate formats, pseudonym policies, and message security according to IEEE 1609.2. If C-V2X aligns with these standards, it is feasible for both technologies to use the same PKI infrastructure and certificate provisioning mechanisms. However, practical realization of this scenario requires alignment of security profiles, certificate usage rules, and pseudonym strategies between the two technologies.

Current efforts by organizations such as ETSI[28] (https://www.etsi.org/committee/its) and the 5G Automotive Association (5GAA), in collaboration with the European Commission, aim to bridge these gaps and ensure consistent handling of cryptographic credentials and message security across both technologies. One notable harmonization initiative is the C-V2X Plugtest events[29], organized by ETSI in partnership with 5GAA. Once the harmonization efforts mature and are reflected in updated conformity assessments and policy documents, stakeholders should be able to deploy hybrid C-ITS services that are fully interoperable and secured under a unified PKI trust model within the EU framework.

Regardless of the uncertainties and challenges related to the harmonization of communication technologies, the implementation of C-ITS communication technology carries a set of strategic, technical, and operational implications. NRAs are not just passive users of technology; they are trust anchors, infrastructure providers, and service facilitators. To fulfil these roles effectively, several key considerations should be taken into account:

1. **Infrastructure Planning and Investment:** Short-range communication, whether through DSRC or C-V2X PC5, requires a dense network of roadside units (RSUs) for certain services to function effectively. Road operators must evaluate traffic patterns, safety-critical zones (e.g. intersections, tunnels), and urban-rural coverage trade-offs to determine where to invest in short-range infrastructure. Cellular-based C-V2X (Uu interface) may reduce hardware requirements, but critical services with latency

[27] C-ITS Security & Governance. C-Roads platform, Working Group 2, Task Force 1. Version 2.2.0, 28.05.2024
[28] ETSI has a dedicated "Technical Committee" for ITS (https://www.etsi.org/committee/its)
[29] https://www.etsi.org/events/2360-cv2x-plugtests-4

constraints still depend on localized communication infrastructure. A hybrid strategy should be tailored to each region's topology and service needs.

2. **Service Authorization and Role Management:** C-ITS services rely on role-based access control managed through IEEE 1609.2 certificates. Road authorities, as service enablers and often policy enforcers, must define clear operational roles (e.g. emergency services, road maintenance vehicles) and ensure that the corresponding service-specific permissions (SSPs) are accurately provisioned. This involves coordination with Certificate Authorities (CAs) to ensure that roles are reflected in the authorization structure and that only legitimate actors can access sensitive or privileged services.
3. **Trust Model Participation and PKI Governance:** Engagement with the European Certificate and Trust List (ECTL) and compliance with EU CCMS requirements is essential for participation in the federated trust model. Road authorities must understand and align with the certificate policy (ETSI TS 103 097) and ensure their organizational PKI (or the PKI of their service providers) is certified for the intended services. This includes decisions on whether to join existing trust hierarchies or establish their own CAs for regional control.
4. **Security Operations and Lifecycle Management:** Managing IEEE 1609.2 and X.509 certificates requires robust operational processes, including certificate issuance, revocation, and renewal. Authorities must have processes in place to detect and respond to misuse, maintain privacy (e.g. pseudonym rotation), and support failover scenarios. This demands significant coordination with national or regional PKI providers and may require establishing internal teams or outsourcing operations to qualified Trusted Service Providers (TSPs).
5. **Interoperability and Compliance Strategies:** Authorities deploying C-ITS services must plan for cross-border and multi-vendor interoperability. This requires ensuring that the communication infrastructure (including PKI) are interoperable with EU-wide specifications, and that services are designed to be resilient to differences in underlying technologies (e.g. DSRC vs C-V2X). This also includes adherence to data protection laws and privacy guidelines, especially regarding pseudonymity and the handling of identifiable data in backend systems.
6. **Stakeholder Coordination and Policy Alignment:** C-ITS deployment is inherently multi-stakeholder. Authorities must coordinate with OEMs, telecom operators, local municipalities, and emergency services to ensure alignment on service priorities, technical interfaces, and trust relationships. This includes ensuring backend systems are secured (typically via TLS/X.509), but also determining which backend services require certification or PKI integration, and which can remain outside the EU CCMS trust model.
7. **Operational Readiness and Incident Response:** Authorities must be ready to handle security incidents, certificate misuse, or communication failures. This includes monitoring and logging communication events, participating in PKI incident response mechanisms, and ensuring that fallback mechanisms are in place for safety-critical services. Operational readiness also extends to training staff and integrating C-ITS operations into existing traffic management centres.

A possible alternative to the harmonization and coexistence of ITS-G5 and C-V2X-based services is that only one of the technologies is used, but this scenario has not received much

attention in this project. It is however worth noting that there is a significant trend towards C-V2X preference in other areas of the world, and countries such as the US, Japan and South Korea have committed to C-V2X as their primary V2X technology. According to some of our informants, a potential future scenario is that Europe may also abandon DSRC/ITS-G5. Such decisions are highly complex and political, and outside the scope of this report. What seems quite certain, however, is that C-V2X will continue to have an important role in European C-ITS communications, and that C-V2X solutions will eventually be aligned and compliant with the EU CCMS requirements.

7.4 Roadmap

The roadmap provides a generic overview of the main phases of the C-ITS PKI implementation. The timing of the different phases will vary from case to case. The deployment plan (Figure 8) sketched by S. Ruehrup et. Al. shows an example of an urban deployment where infrastructure deployment is a starting point and can be used in conjunction with the roadmap. Appendix 1 provides examples of system engineering approaches to C-ITS.

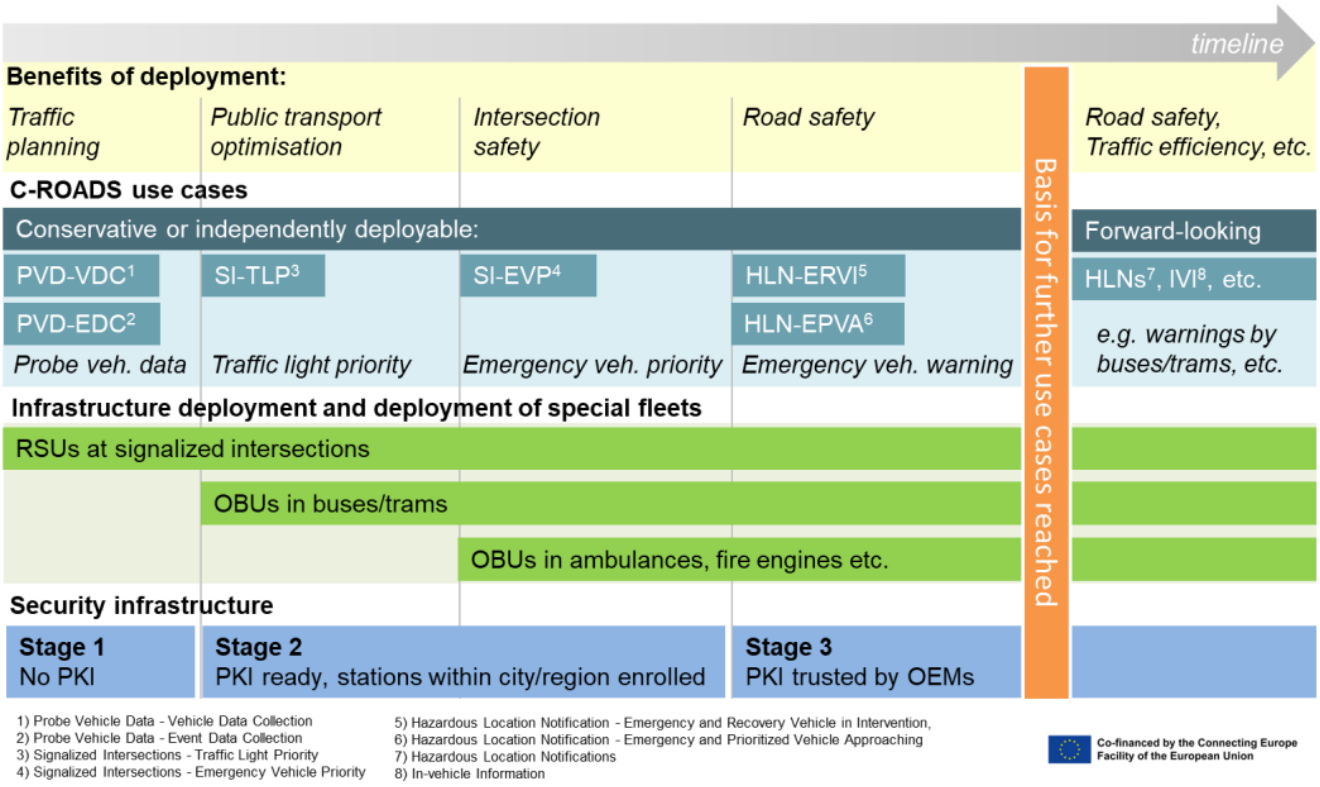

Figure 8:A gradual deployment with increasing support of use cases. From: S.Ruehrup, L. Conceição, J. Montenegro, P. Meckel: "The Chicken and the Egg – Perspectives of C-ITS Deployment", ITS European Congress, 2023.

The PKI-stages presented in Figure 8 are also reflected in the roadmap presented below.

Phase 1: Planning and preparation (Stage 1)

- Define objectives and scope.
- Identify the services to be provided.
- Understand the procurement process and the national procurement procedure.
- Allocate roles and responsibilites. Who are the parties involved? Organisations/teams/third parties.
- Overview of the infrastructure requirements of the services to be provided.
- Communication infrastructure: short range, long range, hybrid?
- ◊Milestone: Complete planning and preparation phase.

Phase 2: Design and development (Stage 1-2)

- Technical specifications.
  - Private keys must be secured.
  - CA and its supporting components must be highly available.
  - Certificate registration procedure must be robust.
  - Authenticate and authorise requests to the CAs.
  - Use a separate intermediate CA per technology or organisation function. Separating CAs in this way will reduce the impact of compromise of a single CA and provide a separation of duty between each CA.
  - Automated certificate renewal.
  - Keep the root CA offline and be unavailable for use. If the root CA were to be compromised, and attacker could gain control of the entire PKI and compromise trust in the entire system, including any sub-systems reliant on the PKI
- Certificate revocation of subordinate CAs.
- Procurement - follow national procurement procedure.
- Pilot testing.
- ◊Milestone: Successful pilot testing and validation of the PKI.

Phase 3: Implementation (Stage 2)

- Infrastructure setup
- Issue certificates

Phase 4: Deployment (Stage 3)

- Full-scale deployment of the PKI
- Perform regular maintenance and updates to the system
- ◊Milestone: Continuous monitoring and improvement of the PKI

The roadmap presented in this section is made specifically for short-lived IEEE 1609.2 certificates and may therefore not be suitable for other purposes.

7.4.1 Phase-specific considerations for NRAs

Below is a more detailed description of key topics and activities which NRAs need to address in the various phases described in the roadmap. These descriptions are generic, and some of the topics and activities suggested may be of varying relevance depending on the use case.

Phase 1: Planning and preparation

This foundational phase helps NRAs clarify what they are trying to achieve, and how.

Defining objectives and scope
At the outset, NRAs need to articulate the goals of their PKI project. What type(s) of C-ITS service(s) will the PKI support? Will it be limited to national use, or will it interface with other countries or EU-level systems? This is also where the intended geographic scope, user base (e.g., vehicles, infrastructure units), and expected growth over time should be roughly estimated.

Understanding the environment and infrastructure
C-ITS services depend on reliable communication channels. NRAs must consider what types of communication infrastructure are available or planned — for instance, short-range (e.g. ITS-G5), long-range (e.g. cellular), or a hybrid approach. This will influence how certificates are used and distributed across the ecosystem.

Procurement and legal readiness
Given that many PKI components (such as Certificate Authorities or Hardware Security Modules) may be provided by external suppliers, NRAs must familiarize themselves with national procurement laws and procedures early on. Procurement planning should align with the expected technical and governance needs of the PKI.

Roles and stakeholders
Establishing a PKI requires involvement from a variety of actors — including national ministries, IT departments, legal experts, and possibly third-party vendors. Early in the process, NRAs should begin mapping out who the key players are, and what roles they might play. For instance, who will be responsible for issuing certificates? Who ensures compliance with EU rules? Who handles day-to-day operations?

Phase 2: Design and development

This is where the high-level ideas from Phase 1 are transformed into detailed designs and working systems.

Designing the PKI architecture
The technical design needs to reflect security, availability and scalability. For example:

- Private keys must be stored securely, typically in Hardware Security Modules (HSMs)
- The Certificate Authority (CA) systems must be resilient to failure or attack – requiring redundancy and monitoring mechanisms
- There must be clearly defined procedures for registering and authorizing certificate requests, to prevent misuse

A layered design is also often recommended. Using intermediate CAs that handle different technologies or organizational functions can limit the impact/consequence if something goes wrong and help ensure separation of duties. For example, having one CA for in-vehicle systems and another for roadside units adds resilience.

Critically, the Root CA, which sits at the top of the trust chain, should be kept offline and only brought online for signing operations. This protects the integrity of the entire PKI.

Certificate management processes
This includes how certificates are issued, renewed, and revoked. Automation of certificate renewal can reduce human error and help scale the system. Revocation mechanisms are essential to invalidate certificates that are no longer trustworthy – whether due to compromise, misbehaviour, or expiry.

Pilot testing and validation
Before anything goes live, pilot testing should be conducted to validate that the system works as expected. This includes technical tests, performance benchmarks, and initial operational procedures. Testing should reflect real-world use cases to ensure confidence in security and reliability.

Procurement execution
This is the phase where actual procurements are likely to occur, based on the designs and specifications developed earlier. It's vital that the procurement process reflects both technical requirements and legal obligations.

Phase 3: Implementation

With a validated design and contracted vendors (and/or internal teams) in place, implementation begins.

Infrastructure setup
The technical components – CAs, Registration Authorities, secure key storage, audit logging systems – are installed, configured, and integrated. At this point, the PKI moves from a plan to a working system.

Operational launch
This is when the first live certificates are issued to authorized devices or actors in the system. These may include vehicles, roadside units, or backend services. The issuance process must follow strict protocols defined during the design phase, ensuring that only legitimate entities receive valid credentials.

Coordination and oversight
Implementation requires close coordination between technical teams, oversight bodies, and any third-party providers. NRAs should ensure that all stakeholders are aligned on procedures, security measures, and escalation paths in case issues arise.

Phase 4: Deployment

With infrastructure in place, the PKI enters full operation, supporting rea-world C-ITS deployments.

Full-scale operation
All systems go live across the intended coverage area. Certificate issuance becomes routine, and operational processes stabilize. The PKI now actively supports secure communications between vehicles, infrastructure, and central systems.

Ongoing maintenance and security
A live PKI is not static. Regular system maintenance, software updates, and security monitoring are needed to keep the infrastructure secure and up-to-date. This includes patching vulnerabilities, rotating keys when needed, and maintaining a functioning incident response process.

Long-term governance and improvement
NRAs must establish clear routines for system oversight, including audits, compliance checks, and reporting. Feedback from operational use – whether technical issues or policy gaps – should feed into a process of continuous improvement.

In summary, implementing a PKI for C-ITS is not just a technical exercise – it's a multi-dimensional undertaking that touches on strategy, technology, procurement, governance, and operations. By approaching the process in structured phases and maintaining a clear understanding of objectives and stakeholder roles, NRAs can establish a robust, secure foundation for enabling future mobility services across Europe.

7.4.2 PKI participants and roles in the trust hierarchy

In addition to the roles and stakeholders mentioned in section 7.4.1, NRAs should also familiarize themselves with the "PKI participants and roles" defined in section 1.3 of the Certificate Policy. Table 6 provides a summary of these roles, along with likely candidates for the various roles. These roles will all need to be addressed when defining and designing a PKI. Some of the roles are authoritative and uniquely instantiated, while others are operational and can be instantiated by one or more entities.

Table 6: Overview of the main roles in the C-ITS trust model. Orange indicates authoritative roles while blue indicates operational roles

Role	Description	Main responsibilities	Candidates
CPA – C-ITS Certificate Policy Authority	A governing body composed of representatives from key C-ITS stakeholders, responsible for defining and overseeing the certificate policy and	- Maintaining policy documents - PKI authorisation management	Representatives from various stakeholders (member states, vehicle manufacturers, etc.)

Role	Description	Main responsibilities	Candidates
	trust framework for secure communications within the system		
TLM – Trust list manager	Single entity appointed by CPA	- Maintaining and distributing the ECTL, including the list of trusted root CAs	Neutral, trusted entities, such as the European Commission
Accredited PKI auditor	An independent entity which has the necessary accreditation to conduct PKI audits	- Auditing root CAs, TLM and sub-CAs - Providing audit reports and notifying relevant parties about audit results	Independent and competent bodies, recognized by CPA (e.g. accredited audit firms, cybersecurity agencies or government-designated bodies)
CPOC – C-ITS point of contact	Single entity appointed by CPA Central interface for secure communication exchange between all entities of the C-ITS trust model	- Reviewing change requests and recommendations - Receiving registration/enrolment requests - Transmitting root CA certificates to TLM - Publication of ECTL	European Commission, ENISA, other neutral European organizations
Root CA	Top-level certificate authority that anchors trust in the C-ITS trust model	Generate and manage root certificates; ensure secure issuance to subordinate CAs	Cybersecurity authorities, national PKI providers, accredited trust service providers
EA – Enrolment authority	Issues enrolment credentials to C-ITS stations to prove their legitimacy	Validate and process enrolment requests from C-ITS stations; issue enrolment certificates	Cybersecurity service providers, manufacturers with secure credential infrastructure
AA – Authorisation authority	Grants short-term authorization tickets allowing secure message exchange	Issue authorization tickets to certified stations based on enrolment credentials	Cybersecurity service providers, vehicle OEMs, trusted third-party operators
C-ITS station	End entity (vehicle, RSU, etc.) that sends/receives C-ITS messages	Transmit and receive trusted C-ITS messages; use valid authorization tickets	Vehicle OEMs, RSU vendors, public transport vehicles,

Role	Description	Main responsibilities	Candidates
			smart infrastructure devices
Manufacturer	Entity that designs and builds C-ITS stations (hardware and/or software)	Ensure C-ITS station compliance with technical and security requirements	Vehicle OEMs, RSU manufacturers, technology providers
Operator	Entity responsible for deploying and managing C-ITS stations in the field	Operate and maintain C-ITS infrastructure; manage certificate provisioning and updates	National Road Authorities, road operators, municipalities, fleet operators

7.5 Main cost contributors

The deployment of C-ITS services in a secure, standards-compliant way introduces a range of cost drivers for road operators and authorities. These costs are not only financial but also include organizational, operational, and strategic overhead. Understanding these costs early is critical for budgeting, project planning, and stakeholder engagement. Below is a list of main cost drivers related to PKI:

- **Establishing or integrating with a PKI** (especially one aligned with EU CCMS) can involve substantial setup costs
  - Initial legal and policy compliance (e.g., aligning with ETSI TS 103 097 and Certificate Policies)
  - Technical system integration (interfaces for certificate issuance, validation, revocation, etc.)
  - Staff training or procurement of services from qualified providers
- **Ongoing operational costs**
  - Certificate management (issuance, revocation, pseudonym refresh)
  - Audits, compliance reporting, and governance reviews
  - Costs associated with ECTL certification if the authority chooses to become a certificate authority (CA) or manage sub-CAs

In addition to the PKI specific costs, there are also other cost considerations which influence the overall picture, such as:

- Infrastructure deployment and maintenance
- Security operations and monitoring
- Interoperability testing and certification
- Project management and stakeholder coordination
- Internal training programs
- Public communication and awareness

7.6 Guidance on procurement and costs

To implement and operate a nationwide C-ITS PKI that is interoperable within Europe, NRAs must understand not only the technical and organizational requirements, but also the financial implications and procurement options. This section provides guidance based on interview and workshop discussions, and a few known public tenders.

Competence requirements and implementation models

Running a nationwide PKI requires a high level of IT competence, especially in the areas of cryptography, infrastructure management, and relevant C-ITS standards and regulations. Additionally, a working knowledge of C-ITS services is critical for aligning PKI operations with the specific requirements of connected vehicle systems.

There are three main options for PKI implementation:

- **Full in-house operation:** The NRA builds and operates the PKI entirely within its own organization
- **Full outsourcing:** The PKI is purchased as a complete managed service from a vendor
- **Partial outsourcing:** The PKI is developed in collaboration with a vendor, with operations shared between the parties

Regardless of the implementation model, NRAs must undertake preparatory work, including understanding the relevant certificate policies, trust models (e.g. ECTL), and operational service levels.

Cost factors

The cost of setting up and operating a C-ITS PKI varies significantly based on several factors:

- **Scale:** Number of users, vehicles and RSUs supported
- **Complexity:** Number and type of services, interfaces, and certificate types
- **Compliance:** Requirements for audits, reporting, and alignment with ECTL
- **Support requirements:** SLAs, incident response, and redundancy

The costs can be grouped into three broad categories, as shown in Table 7.

Table 7: Main cost categories and recommendations

Type of cost	Description	Recommendations
Initial setup costs	Includes planning, hardware/software, integration, configuration, and testing	• Keep system design and service scope as simple as possible to reduce complexity • Reuse existing infrastructure where feasible (e.g. eIDAS components, government data centers) • Clearly define requirements early to avoid costly change orders • Consider cloud-native or hybrid deployment models to reduce CAPEX

Type of cost	Description	Recommendations
		• Request modular or phased delivery in tenders to maintain flexibility
Operational costs	Ongoing costs for maintenance, certificate lifecycle management, monitoring, support, auditing, and upgrades	• Align operational practices with existing structures to avoid redundant procedures • Define service level agreements (SLAs) carefully to balance availability with cost • Use automation for certificate issuance and revocation wherever possible • Consider multi-year contracts to stabilize operating costs • Explore outsourcing options to vendors already experienced with C-ITS PKI
Infrastructure upgrades	Costs for upgrading or replacing obsolete hardware or systems, e.g. due to rapid C-ITS technology evolution	• Favour virtualized or cloud-based services to reduce hardware refresh frequency • Build refresh cycles into long-term budgeting from the start • Select scalable, vendor-independent solutions to avoid vendor lock-in • Plan for standards evolution (e.g. new security protocols, certificate formats) • Monitor system use to avoid over-provisioning hardware or services

Benchmark costs from existing tenders

To support more informed planning, we have attempted to gather cost benchmarks from real-world procurement examples. Unfortunately, our efforts have only produced two concrete examples:

- EU C-ITS Root Certification Authority (2019): Initial setup cost was approximately €1 million, with annual operations at €400,000, subject to variation based on system size and user base[30].
- Microsec contract with German Autobahn (2022): Provided PKI services for V2X for a 4-year period. The estimated contract value was €825,000[31]

In addition to these data points, we anticipate that the costs associated with pilot-scale test environments will be considerably lower. Table 8 provides an indicative overview of expected cost ranges for C-ITS PKI solutions at various scales. However, it is important to emphasize that these figures are highly uncertain and derived from a very limited dataset. Actual costs will vary depending on factors such as the number of certificates issued, security requirements, geographic scope, and the degree of integration with national infrastructure. To supplement this information, NRAs are encouraged to consult relevant tenders published on the EU TED portal for additional benchmarking insights.

[30] https://teskalabs.com/blog/meili-c-its-pki-as-a-service
[31] https://bbj.hu/business/industry/deals/microsec-wins-contract-from-german-motorway-operator/

Table 8: Cost range estimates for C-ITS PKIs

Scale	Estimated setup cost	Estimated annual operating cost
Pilot/local deployment	€ 200,000 – € 400,000	€ 100,000 – € 200,000
National deployment	€ 500,000 – € 1,000,000	€ 200,000 – € 400,000
EU-level root CA	~ € 1,000,000	~ € 400,000

Procurement process recommendations

To obtain realistic and tailored estimates, NRAs are advised to:

- **Issue a Request for Information (RFI):** Engage the market early by outlining functional requirements, expected certificate volumes, and intended service levels. Solicit input from vendors on feasibility and cost structures.
- **Review existing tenders on the EU TED portal:** These can provide valuable insights into both cost and specification details.
- **Pilot first, then scale:** Consider phased deployment strategies to validate operational models and cost assumptions before national rollout.
- **Request Total Cost of Ownership (TCO):** When procuring, ask vendors to submit pricing based on a 5- or 10-year operational model to account for long-term sustainability.
- **Explore shared or regional approaches:** Where feasible, NRAs could consider collaborative models to share infrastructure or administrative overhead.

Final considerations

Managing a C-ITS PKI is a long-term commitment, and decisions made during procurement can significantly affect both the cost and success of the initiative. Realistic budgeting should account for evolving standards, certificate policy updates, and system scaling. NRAs should also ensure internal capacity to interact with and supervise vendors, and to validate PKI compliance with European frameworks such as the EU CCMS.

8 D2.2 Conclusions

This chapter concludes our work by summarizing and reflecting on the main findings and guidance presented throughout the report. In particular, it revisits the key recommendations introduced at the beginning of Chapter 7 and elaborates on their practical implications for National Road Authorities (NRAs) tasked with implementing C-ITS PKIs. These reflections are grounded in stakeholder interviews, workshops, and literature reviewed during the project.

While the recommendations presented here draw from a broad and representative body of input, they are not intended as definitive solutions. Their feasibility, relevance, and impact will vary based on the specific national, legal, and institutional contexts in which they are applied. C-ITS PKI deployment is a complex and strategic undertaking that requires careful tailoring to local conditions. These recommendations should therefore be seen as guiding principles - supporting informed decision-making and adaptation - rather than prescriptive instructions.

8.1 Key recommendations and reflections

Table 9 provides a more comprehensive summary of the generic recommendations from Table 5 in section 7.1, along with an indication of their relevance for the different phase(s) in the roadmap presented in section 7.4.

Table 9: Key recommendations for NRAs implementing C-ITS PKI. "L" indicates low relevance, "M" indicates medium relevance and "H" indicates high relevance

Recommendation	Roadmap phase			
	1	2	3	4
Hire skilled resources The successful design and operation of a C-ITS PKI depend heavily on the availability of personnel with expertise in cryptography, PKI infrastructure, and C-ITS standards such as IEEE 1609.2 and ETSI TS 103 097. Given that such expertise is rare in many public-sector contexts, NRAs are encouraged to invest in specialized recruitment, structured training, or strategic partnerships with external experts to ensure operational competence.	H	H	M	L
Conduct regular audits Continuous verification of PKI performance and compliance is essential for maintaining trust and operational integrity. Regular audits – ideally by accredited third parties – should be embedded into routine processes to ensure alignment with EU CCMS requirements and to identify issues before they become critical.	L	M	H	H
Establish a community/forum for NRA representatives The establishment of a dedicated forum for NRA representatives responsible for C-ITS PKIs would provide a valuable platform for collaboration, knowledge sharing, and alignment on technical and policy issues. Such a community could organize joint workshops,	H	M	M	L

Recommendation	Roadmap phase			
	1	2	3	4
training programs, and working groups to collectively advance implementation maturity across Europe.				
Promote open standards at the EU level The use of open, non-proprietary standards is crucial for reducing dependency on patented technologies, lowering costs, and enhancing interoperability. NRAs and EU bodies should actively support the adoption and promotion of open standards across all layers of the C-ITS technology stack, including PKI components.	H	M	L	L
Leverage managed PKI services Given the technical complexity and ongoing maintenance demands of C-ITS PKI, NRAs may benefit from outsourcing parts of the PKI lifecycle to Trusted Service Providers. Managed services can offer operational efficiency, access to specialist expertise, and alignment with evolving security requirements, especially for NRAs lacking internal capacity.	M	H	H	H
Enhance supplier collaboration and utilize automation Strong supplier relationships, combined with effective use of automation, can significantly streamline PKI operations. Automated processes for certificate issuance, revocation, and renewal reduce the risk of human error and enable scalability. Clear expectations around standards compliance and security policies should be established in procurement contracts and operational frameworks.	M	H	H	H
Establish/participate in C-ITS interest groups In addition to internal coordination, NRAs should engage in broader C-ITS interest groups that include OEMs, telecom operators, municipalities, and technology vendors. These platforms enable alignment on technical specifications, policy requirements, and interoperability challenges, facilitating smoother deployment and governance.	H	H	M	L
Adhere to the EU standard for C-ITS PKI Compliance with the EU Certificate and Trust Model, particularly ETSI TS 103 097, is vital for interoperability across national borders. NRAs must ensure that their PKI architectures, certificate formats, and operational procedures align with EU-wide specifications to participate effectively in the federated trust model.	M	H	H	H
Use the EU C-ITS PKI for cross-border data exchange To enable secure, seamless communication between vehicles and infrastructure across EU countries, integration with the EU C-ITS PKI can be beneficial. This ensures that trust is preserved when vehicles cross borders and that messages can be authenticated regardless of jurisdiction.	L	M	H	H
Apply adequate monitoring and conduct regular security audits	L	M	H	H

Recommendation	Roadmap phase			
	1	2	3	4
PKI systems must be continuously monitored for signs of misuse, technical faults, or compromise. NRAs should implement real-time monitoring tools, establish robust alerting systems, and maintain an ongoing program of internal and external security audits to detect and address issues before they impact service reliability.				
Foster stakeholder collaboration and strategic planning C-ITS deployments involve a wide range of stakeholders, each with distinct roles and priorities. NRAs are advised to engage in proactive and sustained collaboration across the ecosystem – including vehicle manufacturers, telecom providers, municipal governments, and emergency services – through both strategic planning and joint policy development.	H	H	M	M
Encourage public-private collaboration NRAs are encouraged to form partnerships with private sector actors to share costs, pool expertise, and reduce time-to-market. Public-private collaboration can be particularly valuable in areas such as infrastructure deployment, system integration, and backend services, where economies of scale and shared investments can yield mutual benefits.	H	M	H	M
Invest in scalable and flexible infrastructure Future C-ITS services will likely evolve in scope and complexity. It is therefore essential that infrastructure investments support modularity, scalability, and adaptability to emerging standards. Virtualization, cloud-native architectures, and vendor-neutral solutions can help ensure long-term flexibility and sustainability.	H	H	H	H
Ensure backwards compatibility when feasible Given the coexistence of legacy systems and evolving technologies, NRAs should consider maintaining backwards compatibility wherever feasible. This can facilitate gradual rollouts, avoid unnecessary obsolescence, and support smoother transitions between system generations.	M	M	H	H
Develop mature, commercially viable products For C-ITS to succeed, the products and services offered must be reliable, user-friendly, and economically viable. NRAs should support the development of mature, production-ready services and engage with end users early to understand their needs and ensure uptake. Clear commercialization pathways are essential for private sector involvement and sustained innovation.	M	M	H	H
Support good collaboration between C-ITS providers Interoperability and end-user trust depend on coordination between different C-ITS providers. Joint testing environments, interoperability pilots, and shared trust frameworks are essential tools for ensuring	M	M	H	H

Recommendation	Roadmap phase			
	1	2	3	4
seamless service integration and maintaining a cohesive European ecosystem.				

8.2 Additional considerations

Table 10 lists a set of additional considerations, along with an indication of their relevance for the different phase(s) in the roadmap presented in section 7.4.

Table 10: Additional considerations for NRAs implementing C-ITS PKI. "L" indicates low relevance, "M" indicates medium relevance and "H" indicates high relevance

Recommendation	Roadmap phase			
	1	2	3	4
Operational readiness and incident response Beyond implementation, NRAs must be prepared for real-time operational scenarios, including certificate misuse, communication failures, and cybersecurity incidents. This calls for well-defined incident response protocols, real-time monitoring and alerting systems, and the integration of PKI oversight into national traffic management and emergency coordination infrastructures.	L	M	H	H
Governance roles and participation in the EU trust model NRAs have a dual role as implementers and trust anchors within the EU's federated C-ITS framework. Active participation in the EU trust model requires legal alignment, technical readiness, and possibly the establishment or oversight of national Root or Intermediate Certificate Authorities. These strategic decisions carry long-term implications for control, scalability, and compliance.	H	H	M	M
Phased deployment and lifecycle management A structured deployment roadmap, progressing from planning through design, testing, and deployment, allows NRAs to manage complexity and risk. Lifecycle management practices – particularly around certificate issuance, renewal, and revocation – must be embedded from the outset to ensure the sustainability and security of the trust infrastructure over time.	H	H	H	H
Cost considerations and procurement strategy C-ITS PKI deployment introduces significant costs, including setup, operation, and future upgrades. NRAs are advised to conduct early market engagement through RFIs, define clear and modular procurement specifications, and explore shared service models where feasible. Piloting before scaling and requesting total cost of ownership estimates can help control long-term expenditures.	H	H	M	M

Recommendation	Roadmap phase			
	1	2	3	4
Hybrid communication technologies and technical flexibility C-ITS systems increasingly rely on hybrid communication models—combining short-range (e.g. ITS-G5 or C-V2X PC5) and long-range (e.g. cellular) technologies. Each has unique implications for security and certificate usage. NRAs must ensure that their PKI infrastructures are sufficiently flexible to support both IEEE 1609.2 and X.509 models, in accordance with relevant EU standards.	H	H	H	H

References

ARINC. (2014, January 2). *ARINC Report 835-1: Guidance for Security of Loadable Software Parts Using Digital Signatures*. https://aviation-ia.sae-itc.com/standards/arinc835-1-arinc-report-835-1-guidance-security-loadable-software-parts-using-digital-signatures

ARINC. (2018). *ARINC 842 Guidance for usage of digital certificates*.

ATA. (2020). *Spec 42: Aviation Industry Standards for Digital Information Security*. https://publications.airlines.org/CommerceProductDetail.aspx?Product=294

Bernsmed, K., Fr, C., Meland, P. H., & Myrvoll, T. A. (2017). Security requirements for SATCOM datalink systems for future air traffic management. *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, 1–10. https://ieeexplore.ieee.org/abstract/document/8102083/?casa_token=MV4lJaXKuXYAAAAA:7OxuSvUjG8iLPXjQ5stwvtw_P2xSMcoUcgOs9xR1ZiL9hSECJB-2OkyePyqKo3kEgwDMAiyorc1A

Callan, T. (2021, August 2). Top 5 Public Key Infrastructure (PKI) Pitfalls and How to Overcome Them—Spiceworks. *Spiceworks Inc*. https://www.spiceworks.com/it-security/security-general/guest-article/top-5-public-key-infrastructure-pki-pitfalls-and-how-to-overcome-them/

C-Roads. (2023). *Annual pilot overview report 2022*. C-Roads. https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/Annual_pilot_overview_report_2022.pdf

C-Roads. (2024). *C-ITS Roadmap*. C-Roads. https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/C-ROADS_C-ITS_Roadmap_v1.0.pdf

Ellison, C., & Schneier, B. (2000). Ten risks of PKI: What you're not being told about public key infrastructure. *Comput Secur J*, *16*(1), 1–7.

ETSI. (2020). *ETSI EN 302 663—ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band* (Version V1.3.1).

https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf

EU. (2024a, April 4). *eIDAS Regulation | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

EU. (2024b, May 21). *European Digital Identity (EUDI) Regulation | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation

Frøystad, C., Bernsmed, K., & Meland, P. H. (2017). Protecting Future Maritime Communication. *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3098954.3103169

Frøystad, C., Bernsmed, K., Meland, P. H., Rødseth, Ø. J., & Nesheim, D. A. (2017). *D2. 2 Using digital signatures in the maritime domain*. CySIMS-SE. https://nfas.autonomous-ship.org/wp-content/uploads/2020/09/cysims-d22.pdf

Gritzalis, S. (2005). A good-practice guidance on the use of PKI services in the public sector of the European Union member states. *Information Management & Computer Security*, *13*(5), 379–398.

Guida, R., Stahl, R., Bunt, T., Secrest, G., & Moorcones, J. (2004). Deploying and using public key technology: Lessons learned in real life. *IEEE Security & Privacy*, *2*(4), 67–71.

Gutmann, P. (2002). PKI: It's not dead, just resting. *Computer*, *35*(8), 41–49.

Hadan, H., Serrano, N., & Camp, L. J. (2021). A holistic analysis of web-based public key infrastructure failures: Comparing experts' perceptions and real-world incidents. *Journal of Cybersecurity*, *7*(1), tyab025. https://doi.org/10.1093/cybsec/tyab025

Hermann, J. (2001). Overview of PKI progress in Higher Education. *Library Hi Tech News*, *18*(1). https://doi.org/10.1108/lhtn.2001.23918aac.013

ISO. (2018). *ISO 21188:2018 Public key infrastructure for financial services—Practices and policy framework*. ISO. https://www.iso.org/standard/63134.html

Joint Research Centre. (2023). *Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*. European Commission.

https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0._20230916.pdf

Joint Research Centre. (2024). *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*. European Commission. https://cpoc.jrc.ec.europa.eu/data/documents/E01941_C-ITS_Certificate_Policy_Release_3_0_FINAL.pdf

Linden, M., Linna, P., Kivilompolo, M., & Kanner, J. (2002). Lessons learned in PKI implementation in higher education. *Proceedings of EUNIS2002, the 8th International Conference of European University Information Systems, Portugal*, 246–251. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7f925ae8e52e2f79e87ba17b9975daddb051078a

Mantas, G., Lymberopoulos, D., & Komninos, N. (2012). PKI Security in Large-Scale Healthcare Networks. *Journal of Medical Systems*, *36*(3), 1107–1116. https://doi.org/10.1007/s10916-010-9573-1

McKinnon, J. (2022). The Most Popular SSL Certificate Authorities Reviewed (2022). *WPMU DEV Blog*. https://wpmudev.com/blog/ssl-certificate-authorities-reviewed/

Patterson, P. (n.d.). *PKI deployment in the Aerospace Industry*. Retrieved 27 June 2024, from https://www.icao.int/safety/acp/ACPWGF/ACP-WG-I-6/ACP-WGI06-IP03-ICAO-CertiPath-DSWG-PKI-Presentation.ppt

Payne, G., & Payne, J. (2004). *Key concepts in social research*. https://doi.org/10.4135/9781849209397

Ponemon. (2020). *The Impact of Unsecured Digital Identities*. Ponemon Institute. https://www.keyfactor.com/resources/content/the-impact-of-unsecured-digital-identities-2020-report-critical-trust-index

Ramadan, M., Du, G., Li, F., & Xu, C. (2016). A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems. *Symmetry*, *8*(9), Article 9. https://doi.org/10.3390/sym8090085

Rødseth, Ø. J., Meland, P. H., Frøystad, C., & Drugan, O. V. (2018). PKI vs. Blockchain when Securing Maritime Operations. *European Journal of Navigation*, *18*(3), 4–11.

Shan, L. (2019). *State-of-the-art Analysis and Applicability of Standards*. https://secredas-project.eu/wp-content/uploads/2017/01/SECREDAS-D10-2.pdf

Appendix A Interview Guide

Time frame:
1 hour

Introduction: 10 min
Short round of introductions

Introduction to the project and the purpose of the interview (this includes information regarding data collection and handling/management) – Clarify what we mean by PKI if that is unclear (maybe "certificate policy" is a better term)

Any questions regarding the project or the interview?

(Questions marked in yellow are most important)

Main part: 45 min
Organizational:

- General status on PKI in [country]?
  - Are you operating your own national root CA or using the European Certificate Authority (EU root CA)?
  - Who is the Enrolment Authority?
  - Who is the Authentication Authority
  - Are there parallel PKIs in your country? (private/public)
  - Number of C-ITS Stations
  - Type of information and messages (roadside, aggregated, broadcast, V2V)
- View on the European level?
- Which paths have you chosen to implement C-ITS Delegated regulation? (Not a regulation!)
- How to connect with the European solution?
- Are you in contact with other NRAs? Which?
- What are the agreements and disagreements?
- Current operations in [country]
  - Who is managing the PKI (issuing certificates)?
  - Reasons for this choice?
  - Tender/competition? Costs public information? Can we get access to this (at a later stage)?
  - Alternatives?
  - Permanent?
  - Problems/challenges with this solution?
- How is enrollment (and revocation) managed?
  - How is the process of enrolling new devices/stations in the security "ecosystem" (PKI)?
- Pilots in [country]?
  - Include certificates and signed data?
- Have you had pilots with other countries?
  - Cross-border
  - Data sharing?
- Conflict of interests?

  - Car manufacturers
  - Telco operators
  - countries

- What is your organization's "role" regarding PKI in C-ITS applications?
  - What roles and responsibilities belong to other organisations?
- PKI competence and resources
  - Support: Are any PKI related responsibilities outsourced, or is everything handled by "in-house" resources?
  - How many people are responsible/working with PKI?
- What have you learnt about operating a PKI?
  - What issues and problems have you encountered when developing and implementing the PKI?
  - What has worked well in your case?
- What actors are involved, and which role do they have?
  - Political, supplier, telco operators, police, etc.
- Politics:
  - What are the challenges? What are the discussions about?

Compatibility and collaboration:

- Are they aware of the situation in Europe? Do they collaborate with other countries?
- How is the compatibility between bordering countries?
- How is the collaboration between countries and road authorities?
  - (Agreements on what certificate standards and key lengths to use?)
  - Agreements regarding roles and responsibilities, including Certificate Authority (CA) role(s)?
- Other things?

Costs:

- Can you say something about the resources required to run a PKI infrastructure?
  - How do the cost and computational requirements scale?
  - What are the resources required to run the administration for certificate and key management?
  - Costs related to customer/user support?
- Any known or expected technological developments which may render present solutions obsolete and introduce extra cost?

Conclusion: 5 min

Thank you for participating in the interview.
Any final questions or remarks?

Appendix B **Systems Engineering Approaches to C-ITS**

The objective of this section is to highlight some of the fundamental principles of system engineering that can be employed during the development the PKI system. Systems engineering is an interdisciplinary approach to enable the realisation of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem. Systems Engineering considers both the business and technical needs of all customers with the goal of providing a quality product that meets the user's needs. [INCOSE Definition]

The development and procurement of any complex system needs to adopt a rigorous and robust methodology to capture the system architecture, describe how it can be implemented, as well as how to maintain, operate and dispose. These concepts are generally captured in in system life cycle and described using ISO15288, see Figure 2

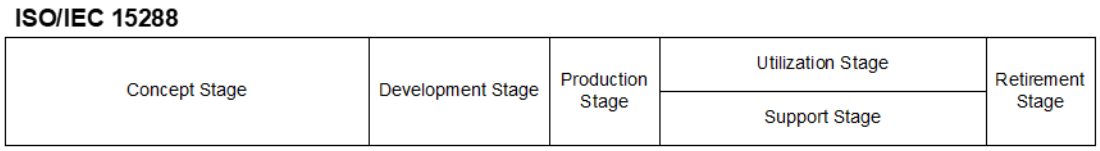

Figure 9: Systems Lifecycle

There are many variations of systems lifecycles from the simple linear process shown in Figure 2 to agile developments that employ iterative V cycles (see Figure 3).

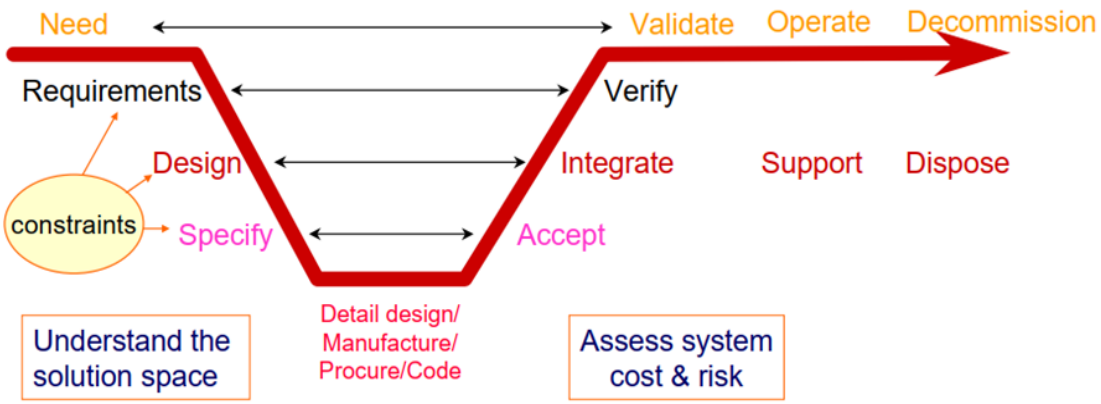

Figure 10 : Systems V cycle.

The NRA will need to develop a PKI that is compatible with both national and European standards as well as many legal and ethical requirements. It is important that all stakeholder requirements are captured and are traceable to the final implementation proving that these have addressed and demonstrated by a process of testing and verification.

It is expected that most NRAs will have a defined systems development process that captures these fundamental stages. These normally are qualified by an external QA assessment. However, it is also possible that some NRAs do not undertake any development rather acting as the pure system operator and outsourcing the development, maintenance and disposal activities for their systems. However, in order to procure a complex system, the basic artefacts of the system engineering process need to be produced, maintained, verified, and validated. The NRA will therefore be required to undertake a concept phase that includes a requirement definition process, followed by requirements analysis and potentially a system architecture design process. This then could be followed by a procurement and contract management process with final implementation, operation and being outsourced to a suitable vendor. It is recommended that if the concept phase is outsource it should include contractual constraints to ensure fair competition.

Concept Stage

A simplified concept stage is outlined in the section below to illustrate some of the outputs required to drive the system development/procurement.

Requirements definition process

The purpose of the requirements definition process is to identify stakeholders. elicit their requirements (including any critical and desired performance constraints) and analysis these for completeness and consistency and establish a validation criterion.

Requirements Analysis process

The purpose of this processes is to establish the system boundary and external interfaces. It needs to establish architectural constraints and derive system requirements including any nonfunctional requirements and also define the system verification criteria.

Architecture Design Process

The final process of the concept phase is to undertake an architecture design process. In this process the logical architecture of the system is defined along with a proposed solution(s). This could also include sub system requirements and the verification and integration concept. The Architecture Design Process is concerned with the synthesis of a solution that satisfies the System Requirements, typically by decomposing the system into a number of sub-systems. It can be applied recursively, first addressing the system-of-interest as part of a wider system (the so-called ‘Systems-of-systems’ perspective) before decomposing the system-of-interest itself.

Typical Outputs

- System Boundary Definition (later incorporated into the System Design Specification)
- External Interface Control Documents
- Logical Architecture (captured within an architectural description where architecture modelling is employed on a project, and also included in the System Design Specification)
- Assessment/Evaluation Reports

- System Design Specification (which captures the mapping of the Logical Architecture onto the realisable sub-systems, modules, and components of the Physical Architecture identifiable as Configuration Items)
- Internal Interface Control Documents
- Sub-system Design Specifications

This process may be supported by an Architectural Trade-off analysis where alternative architecture approaches are identified and then assessed

Enterprise architecture frameworks

A system architecture can be captured and modelled using an enterprise architectural framework. An architectural framework is a robust and consistent way of describing architecture elements using different viewpoints from different stakeholders. These processes were originally developed for large software developments but now have evolved into standardised processes that can represent large scale systems or even systems of systems. Architecture modelling supports the elicitation and understanding of requirement and their impact on potential solutions. ISO/IEC/IEEE 42010 describes an architecture framework as: "The conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders"

There are a number of architecture frameworks commonly in use. These include.:

- DODAF – Department of Defence Architecture Framework
- NAF – NATO Architecture Framework
- TOGAF – The Open Group Architecture Framework
- Zachman Framework
- CVRIA – Connected Vehicle Reference Implementation Architecture

Each of these allow the organisation to development a set of viewpoints that illustrate the requirements, solutions, non-operation requirements such as standard/ regulatory compliance as well as acquisition processes in a coherent and detailed manner.

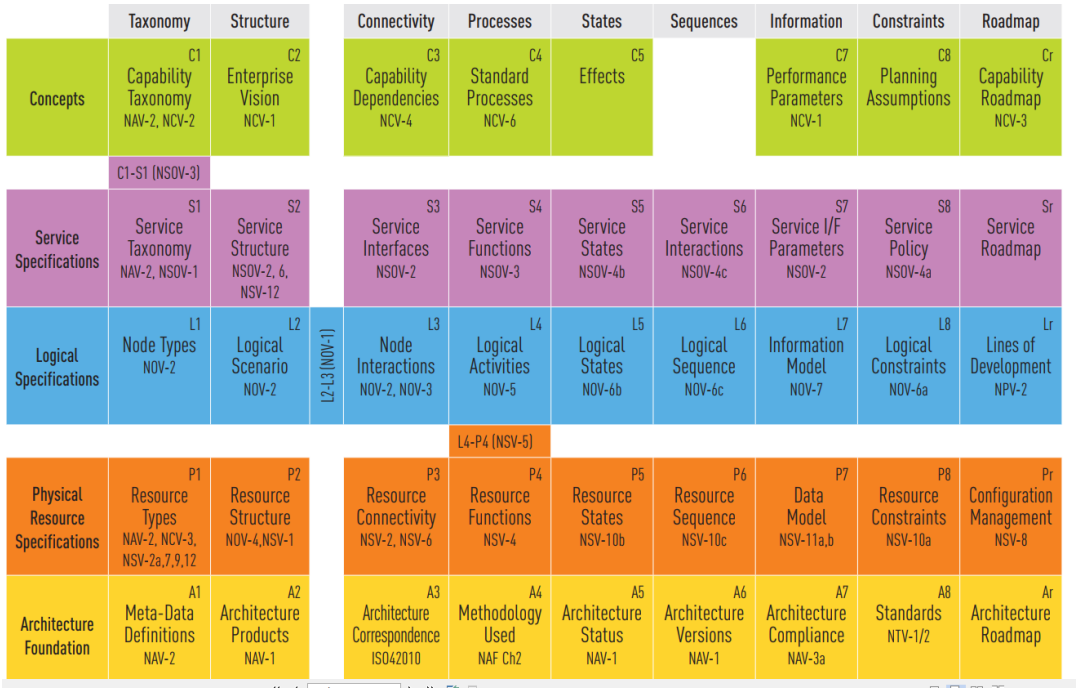

Figure 11 : NAF Viewpoint

Figure 4 has been provided to illustrate the level of detail available in mature AF and at first sight it can seem overwhelming. However, the ITS domain has been active in producing architectures that are relevant to this domain such as ARC-IT

- Viewpoints and Views
- ITS Services / Service Packages
- Physical View
- Physical Objects
- Information Flows
- Functional Objects
- Functional View
- Enterprise View
- Communications View

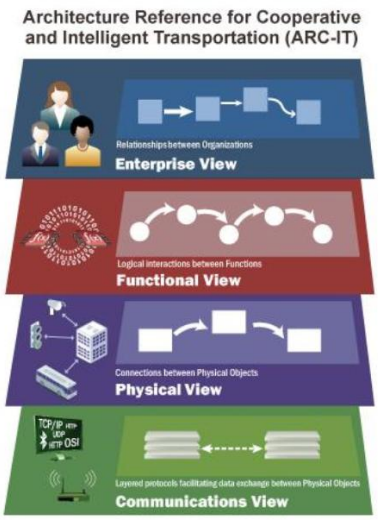

Figure 12 : ARC-IT CVRIA

It is common for an organisation along with their supply chain partners to develop specific architectural frameworks to allow systems operating in domain to support inter-operation using common definition and terms. These can be built from TOGAF employing conceptual models based in ISO42010 and modelled using tools such as ArchiMate. This section provides a brief introduction to the tools and processes used to model the systems architecture and it is

recommended that the NRAs reviews their business model to help identify their optimum approach. It is recommended that the NAT adopt a rigorous system development methodology compliant to the C-ROADS platform.

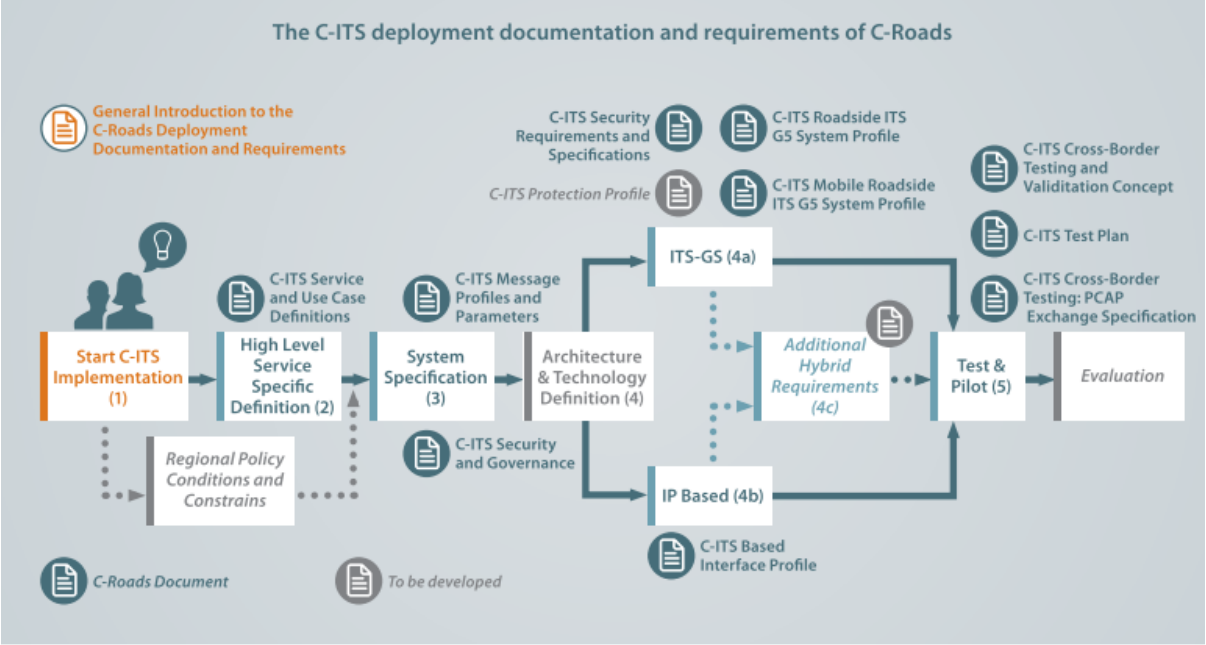

Figure 13 : C-ROADS Process for specification development