TRAFICOM
Finnish Transport and Communications Agency

The implementation model and deployment requirements of the C-ITS system in Finland

Timo Majala, Ville Kilpiö, Jouni Rantanen, Marika Haapajärvi, Lari Väänänen, Jarno Kallio

C-ROADS

Co-funded by
the European Union

Traficom Research Reports
Traficomin tutkimuksia ja selvityksiä
Traficoms forskningsrapporter och utredningar

18/2025

Date of publication
6th June 2025

Title of publication
The implementation model and deployment requirements of the C-ITS system in Finland

Author(s)
Timo Majala, Ville Kilpiö, Jouni Rantanen, Marika Haapajärvi, Lari Väänänen, Jarno Kallio

Commissioned by, date
Finnish Transport and Communications Agency Traficom, 30th May 2024

Publication series and number **Traficom Research Reports 18/2025**	ISSN (e-publication) 2669-8781 ISBN (e-publication) 978-952-311-985-7

Keywords
C-ITS, EU CCMS

Abstract

Cooperative Intelligent Transport Systems (C-ITS) services refer to services that rely on the cooperative exchange of standardised real-time C-ITS messages between vehicles, infrastructure and other road users. They can be implemented via long-range IP networks or short-range communications solutions based on radio technology. In Finland, particular emphasis is placed on long-range solutions. As a core member of the C-Roads Platform – a joint initiative of EU Member States – Finland is committed to complying with the technical specifications adopted by the Platform.

This study sought to identify the European requirements for the national deployment and operation of C-ITS services and to develop a proposal for establishing the necessary capabilities for service deployment. This included consideration of the requirements set by the EU C-ITS security and certificate policies, the EU C-ITS Security Credential Management System (EU CCMS), and the C-Roads Platform regarding the implementation and operation of central C-ITS stations and interchange servers, as well as aspects related to privacy protection. The methods used included a literature review, steering group work, expert interviews and workshops. Valuable contributions also came from consultants, relevant agencies, and the steering group members' own expertise.

Key preconditions identified for the deployment of C-ITS services include the establishment of a national central C-ITS station and interchange server, along with the introduction of certificate services in line with the EU CCMS. It is essential that the operation of C-ITS stations adheres to the information security management requirements defined in the C-ITS security policy. The study examined commercial solutions for central C-ITS stations and interchange servers; however, they were not yet fully compliant with the requirements of the C-ITS security and certificate policies. This was partly due to shortcomings in the C-Roads specifications for long-range communication solutions. Various deployment options were explored, including tailored solution, acquisition of commercial products and open-source development. They all involved certain challenges, and no single solution could be recommended over others. The options should therefore be explored further without delay. Although principles of data and privacy protection are well embedded in C-ITS policies, from a legal standpoint, the grounds for processing personal data remain unclear. Thus, the most straightforward approach would be to begin implementation of C-ITS services with I2V (Infrastructure-to-Vehicle) messages that do not contain personal data. This report includes an implementation plan and recommends the establishment of a coordination group for the development and deployment of C-ITS services to support implementation.

The significance of the study's findings is heightened by their novelty, as there is still limited experience with the application of C-Roads specifications, particularly those related to long-range communication. The shift from pilot projects to full-scale deployment is a timely issue, and the findings of this report support this transition. A key question addressed was whether any requirements or definitions related to C-ITS implementation would hinder the deployment of services in Finland. No elements were identified that would entirely prevent deployment, although a clear recommendation for the implementation of a national central C-ITS station and interchange server could not be made. This will require a more detailed preliminary assessment of the available options and a market survey, as outlined in the implementation plan. The report compiles and interprets European requirements for C-ITS systems and proposes an implementation plan, offering a foundation for the systematic deployment of C-ITS services in Finland.

Contact person Risto Öörni	Language Finnish	Confidence status Public	Pages, total 187
Distributed by Finnish Transport and Communications Agency Traficom	Published by Finnish Transport and Communications Agency Traficom		

Julkaisupäivämäärä
6.6.2025

Julkaisun nimi
C-ITS-järjestelmän toteutusmalli ja käyttöönoton edellytykset Suomessa

Tekijät
Timo Majala, Ville Kilpiö, Jouni Rantanen, Marika Haapajärvi, Lari Väänänen, Jarno Kallio

Toimeksiantaja ja asettamispäivämäärä
Liikenne- ja viestintävirasto Traficom, 30.5.2024

Julkaisusarjan nimi ja numero **Traficomin tutkimuksia ja selvityksiä 18/2025**	ISSN (verkkojulkaisu) 2669-8781 ISBN (verkkojulkaisu) 978-952-311-985-7

Asiasanat
C-ITS, EU CCMS

Tiivistelmä
C-ITS-palveluilla (Cooperative Intelligent Transport Systems) tarkoitetaan älykkäiden liikennejärjestelmien palveluita, jotka toteutetaan vuorovaikutteisesti vaihtamalla standardoituja tosiaikaisia C-ITS-viestejä ajoneuvojen, infrastruktuurin ja muiden tienkäyttäjien kesken. C-ITS-palveluita voidaan toteuttaa pitkän kantaman IP-verkkoihin tai lyhyen kantaman radioteknologiaan perustuvilla tiedonsiirtoratkaisuilla. Suomessa keskitytään erityisesti pitkän kantaman ratkaisuiden hyödyntämiseen. Euroopan jäsenmaiden yhteishankkeen C-Roads Platform ydinjäsenenä Suomi on sitoutunut noudattamaan sen teknisiä spesifikaatioita.

Selvitystyön tavoitteena oli selvittää C-ITS-palveluiden kansalliseen käyttöönottoon ja operointiin liittyvät eurooppalaiset vaatimukset sekä valmistella ehdotus palveluiden käyttöönoton valmiuksien luomiselle. Tähän liittyen työssä huomioitiin C-ITS-keskusyksiköiden ja tiedonvaihtopalvelimien toteutukseen ja operointiin liittyvät EU:n C-ITS-turvallisuus- ja varmennepolitiikkojen, C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) sekä C-Roads-yhteistyöfoorumin asettamat vaatimukset sekä yksityisyyden suojaan liittyvät näkökulmat. Työn tutkimusmenetelminä olivat kirjallisuuskatsaus, ohjausryhmätyö, asiantuntijahaastattelut, työpajatyöskentely sekä tilaajien, toimittajien ja ohjausryhmän asiantuntijaosaamisen hyödyntäminen.

Selvitystyössä tunnistettiin keskeisinä C-ITS-palveluiden käyttöönoton aloittamiseen vaadittavina toimina kansallisen C-ITS-keskusyksikön ja tiedonvaihtopalvelimen sekä C-ITS-turvatunnusten hallintajärjestelmän mukaisten varmennepalveluiden käyttöönotto. C-ITS-yksiköiden operointiin liittyen keskeistä on C-ITS-turvallisuuspolitiikassa asetettujen tietoturvallisuuden hallintaan liittyvien vaatimusten huomioiminen. Työssä tarkasteltiin kaupallisten C-ITS-keskusyksiköiden ja tiedonvaihtopalvelimien ratkaisuja. Ratkaisut eivät vielä olleet täysin C-ITS-turvallisuus- ja varmennepolitiikojen vaatimusten mukaisia, joka osittain johtui pitkän kantaman tiedonsiirtoratkaisuihin liittyvien C-Roads-spesifikaatioiden puutteista. Ratkaisuiden käyttöönottamiseksi tutkittiin erilaisia toteutusvaihtoehtoja, kuten oma räätälöity toteutus, kaupallisen tuotteen hankinta sekä avoimen lähdekoodin yhteisöön perustuva kehittäminen. Kaikkiin ratkaisuista liittyi haasteita eikä pelkästään yhtä vaihtoehtoa voitu yksiselitteisesti nostaa suositeltavaksi. Suosituksena on aloittaa välittömästi eri vaihtoehtojen tarkemmat selvitystyöt. Tieto- ja yksityisyydensuojaan liittyvät periaatteet on laajasti sisällytetty C-ITS-järjestelmän toimintaperiaatteisiin, mutta lainsäädännön näkökulmasta henkilötietojen käsittelyperustetta ei ole yksiselitteisesti osoitettu. Tästä syystä toteutus on selkeintä aloittaa I2V-viesteistä (Infra-to-Vehicle), jotka eivät itsessään sisällä henkilötietoa. Tämä raportti tarjoaa toimeenpanosuunnitelman, jonka tukemiseksi suositellaan myös C-ITS-palveluiden kehityksen ja käyttöönoton koordinointiryhmän perustamista.

Työssä saatujen tulosten merkittävyyttä lisää niiden uutuusarvo, sillä C-Roads-spesifikaatioiden soveltamisesta erityisesti pitkän kantaman tiedonsiirtoon perustuvien ratkaisuiden käyttöönotossa on toistaiseksi vain rajallisesti kokemusta. C-ITS-ratkaisuiden pilotoinnista tuotantovaiheen palveluihin siirtyminen on ajankohtainen teema, jota tämän raportin tulokset tukevat. Tärkeänä tutkimuskysymyksenä oli tunnistaa sisältävätkö C-ITS-toteutukseen liittyvät vaatimukset tai määritelmät esteitä C-ITS-palveluiden käyttöönotolle Suomessa. Käyttöönottoa kokonaan estäviä syitä ei tullut esille, joskin kansallisen C-ITS-keskusyksikön ja tiedonvaihtopalvelimen toteutusmalliksi ei voitu antaa yksiselitteistä ehdotusta. Tämä vaatii tarkemman toimeenpanosuunnitelmassa esitetyn eri vaihtoehtojen esiselvityksen ja markkinakartoituksen. Selvitystyössä toteutettu C-ITS-järjestelmiin liittyvien eurooppalaisten vaatimusten kokoaminen ja tulkinta sekä esitetty toimeenpanosuunnitelma tarjoavat etenemispolun systemaattisen C-ITS-palveluiden käyttöönoton valmistelulle Suomessa.

Yhteyshenkilö Risto Öörni	Raportin kieli suomi	Luottamuksellisuus julkinen	Kokonaissivumäärä 187

Jakaja Liikenne- ja viestintävirasto Traficom	Kustantaja Liikenne- ja viestintävirasto Traficom

Transport- och kommunikationsverket

Utgivningsdatum
6.6.2025

Publikation
Modell för genomförande av ett C-ITS-system och förutsättningar för införande i Finland

Författare
Timo Majala, Ville Kilpiö, Jouni Rantanen, Marika Haapajärvi, Lari Väänänen, Jarno Kallio

Tillsatt av och datum
Transport- och kommunikationsverket Traficom, 30.5.2024

Publikationsseriens namn och nummer **Traficoms forskningsrapporter och utredningar 18/2025**	ISSN (elektronisk publikation) 2669-8781 ISBN (elektronisk publikation) 978-952-311-985-7

Ämnesord
C-ITS, EU CCMS

Sammandrag
Med C-ITS-tjänster (Cooperative Intelligent Transport Systems) avses intelligenta transportsystemtjänster som genomförs interaktivt genom utbyte av standardiserade C-ITS-meddelanden i realtid mellan fordon, infrastruktur och trafikanter. C-ITS-tjänster kan genomföras med dataöverföringslösningar som grundar sig på IP-nät med lång räckvidd eller på radioteknik med kort räckvidd. I Finland fokuserar man särskilt på att utnyttja lösningar med lång räckvidd. Som kärnmedlem i EU-medlemsländernas gemensamma projekt C-Roads Platform har Finland förbundit sig att följa dess tekniska specifikationer.

Syftet med utredningsarbetet var att klargöra de europeiska kraven på det nationella införandet och den nationella driften av C-ITS-tjänster samt att bereda ett förslag till skapande av beredskap för införande av tjänsterna. I arbetet beaktades de krav som C-ITS-centralenheterna och servrarna för datautbyte ställer på genomförandet och driften av EU:s C-ITS-säkerhets- och certifikatpolicyer, de krav som systemet för hantering av C-ITS-säkerhetskoder (EU CCMS) och samarbetsforumet för C-Roads ställer samt synpunkter på integritetsskydd. Forskningsmetoderna i arbetet bestod av litteraturöversikt, styrgruppsarbete, expertintervjuer och workshoppar.

Som centrala åtgärder som krävs för att inleda införande av C-ITS-tjänster identifierades i utredningsarbetet införande av certifikattjänster enligt den nationella C-ITS-centralenheten och servern för datautbyte samt systemet för hantering av C-ITS-säkerhetskoder. När det gäller C-ITS-enheternas verksamhet är det viktigt att ta hänsyn till de krav på hantering av informationssäkerheten som fastställts i C-ITS-säkerhetspolicyn. I arbetet granskades lösningar för kommersiella C-ITS-centralenheter och servrar för datautbyte. Lösningarna var ännu inte helt förenliga med kraven i C-ITS-säkerhets- och certifikatpolicyerna, vilket delvis berodde på brister i C-Roads-specifikationerna för dataöverföringslösningar med lång räckvidd. Olika genomförandealternativ för att införa lösningarna undersöktes, såsom eget skräddarsytt genomförande, anskaffning av en kommersiell produkt samt utveckling baserad på öppen källkod. Alla lösningar var förknippade med utmaningar och det fanns inte ett alternativ som entydigt kunde lyftas fram som rekommendation. Rekommendationen är att omedelbart inleda utförligare utredningar av de olika alternativen. Principer för informations- och integritetsskydd har i stor utsträckning inkluderats i C-ITS-systemets verksamhetsprinciper, men grunden för behandling av personuppgifter har inte entydigt redogjorts för ur lagstiftningsperspektiv. Därför är det tydligast att inleda genomförandet med I2V-meddelanden (Infra-to-Vehicle), som inte innehåller personuppgifter. Denna rapport tillhandahåller en genomförandeplan och som stöd för den rekommenderas också att en samordningsgrupp för utveckling och införande av C-ITS-tjänster inrättas.

Nyhetsvärdet ökar betydelsen av arbetets resultat, eftersom det tills vidare finns endast begränsad erfarenhet av att tillämpa C-Roads-specifikationer särskilt vid införande av lösningar som grundar sig på dataöverföring med lång räckvidd. Övergången från pilotförsök med C-ITS-lösningar till tjänster i produktionsfasen är ett aktuellt tema som stöds av resultaten i denna rapport. En viktig forskningsfråga var att identifiera om kraven eller definitionerna som gäller C-ITS-genomförandet medför hinder för införandet av C-ITS-tjänster i Finland. Omständigheter som helt förhindrar införandet framkom inte, trots att man inte entydigt kunde föreslå en modell för genomförande av en nationell C-ITS-central och server för datautbyte. Detta kräver en utförligare förstudie och marknadskartläggning av de olika alternativen som presenteras i genomförandeplanen. Den sammanställning och tolkning av de europeiska kraven på C-ITS-systemen som genomfördes i utredningsarbetet samt den presenterade genomförandeplanen pekar ut en väg framåt för beredningen av ett systematiskt införande av C-ITS-tjänster i Finland.

Kontaktperson Risto Öörni	Språk finska	Sekretessgrad offentlig	Sidoantal 187

Distribution Transport- och kommunikationsverket Traficom	Förlag Transport- och kommunikationsverket Traficom

FOREWORD

In recent years, research and studies on Cooperative Intelligent Transport Systems (C-ITS) have been conducted in several projects in Finland. These earlier initiatives on C-ITS implementation have analysed the roles of the various stakeholders involved, compared different technologies and explored the potential use of mobile networks in the implementation of C-ITS services. However, they have not attempted to establish a deployment plan for C-ITS services, nor have they examined in detail the preconditions for service deployment in Finland.

The objective of this project was to examine the preconditions for providing C-ITS services in Finland and to develop a proposal for a national implementation model. The work was carried out by a project group comprising Ville Kilpiö from Ramboll Finland Ltd, Jouni Rantanen and Marika Haapajärvi from Sitowise Oy, and Timo Majala, Lari Väänänen and Jarno Kallio from Nodeon Finland Oy. The project was managed by Ville Kilpiö.

The project's progress was monitored by a steering group including Risto Öörni, Mikko Räsänen, Anna Schirokoff, Pekka Pussinen, Ari Kallio and Petri Aarni from the Finnish Transport and Communications Agency Traficom, Petri Antola and Jari Myllärinen from the Finnish Transport Infrastructure Agency, Olli Rossi and Mika Ahvenainen from the traffic management company Fintraffic Road Ltd, Antti Paasilehto from the Ministry of Transport and Communications, Mika Kulmala from the City of Tampere and Niko Kynsijärvi from the City of Helsinki. The steering group was chaired by Risto Öörni. The group supported the project by sharing their expertise with the report's authors and by contributing to quality assurance through comments on the final report.

The views expressed in the final report are those of the authors and do not necessarily reflect the positions of the authority publishing the report or the organisations represented in the steering group.

The study was part of the European C-Roads Extended project, which was co-financed by the Connecting Europe Facility (CEF) in 2024–2027.

The original report was written in Finnish and translated into English.

Helsinki, 6th June 2025

Risto Öörni
Special Adviser
Finnish Transport and Communications Agency Traficom

ALKUSANAT

Yhteistoiminnallisten älyliikenteen järjestelmiin (Cooperative Intelligent Transport systems, C-ITS) liittyvää tutkimus- ja selvitystyötä on tehty useammassa kotimaisessa hankkeessa viime vuosien aikana. Aikaisemmat C-ITS-toteutusta käsittelevät projektit ovat tarkastelleet osapuolten rooleja, vertailleet eri teknologioita ja tarkastelleet mahdollisuutta matkaviestinverkkojen hyödyntämiseen C-ITS-palveluiden toteuttamisessa. Aikaisemmissa kehityshankkeissa ei kuitenkaan ole pyritty muodostamaan suunnitelmaa C-ITS-palveluiden käyttöönotolle tai yksityiskohtaisesti tarkasteltu palveluiden käyttöönoton edellytyksiä Suomessa.

Hankkeen tavoitteena oli tarkastella edellytyksiä C-ITS-palveluiden toteuttamiselle Suomessa sekä valmistella ehdotus C-ITS-palveluiden kansalliseksi toteutusmalliksi. Hankkeen toteuttamisesta vastasi projektiryhmä, johon kuuluivat Ville Kilpiö Ramboll Oy:stä, Jouni Rantanen ja Marika Haapajärvi Sitowise Oy:stä sekä Timo Majala, Lari Väänänen ja Jarno Kallio Nodeon Finland Oy:stä. Työn projektipäällikkönä toimi Ville Kilpiö.

Työn etenemistä valvoi ohjausryhmä, jonka jäseninä toimivat Risto Öörni, Mikko Räsänen, Anna Schirokoff, Pekka Pussinen, Ari Kallio ja Petri Aarni Liikenne- ja viestintävirasto Traficomista, Petri Antola ja Jari Myllärinen Väylävirastosta, Olli Rossi ja Mika Ahvenainen Liikenteenohjausyhtiö Fintraffic Tie Oy:stä, Antti Paasilehto liikenne- ja viestintäministeriöstä, Mika Kulmala Tampereen kaupungilta sekä Niko Kynsijärvi Helsingin kaupungilta. Ohjausryhmän puheenjohtajana toimi Risto Öörni. Ohjausryhmän jäsenet edistivät työn toteutusta jakamalla asiantuntemustaan raportin kirjoittajille työn aikana sekä osallistumalla laadunvarmistukseen kommentoimalla työn loppuraporttia.

Työn loppuraportissa esitetyt näkemykset ovat kirjoittajien omia, eivätkä ne välttämättä edusta raportin julkaisevan viranomaisen tai ohjausryhmässä edustettuina olevien toimijoiden näkemyksiä.

Työ oli osa eurooppalaista C-Roads Extended -hanketta, joka sai Verkkojen Eurooppa -ohjelman (CEF, Connecting Europe Facility) rahoitustukea vuosina 2024–2027.

Alkuperäinen raportti kirjoitettiin suomeksi ja käännettiin englanniksi.

Helsinki, 6. kesäkuuta 2025

Risto Öörni
Erityisasiantuntija
Liikenne- ja viestintävirasto Traficom

FÖRORD

Forsknings- och utredningsarbete i anslutning till intelligenta trafiksystem (Cooperative Intelligent Transport systems, C-ITS) har utförts i flera finländska projekt under de senaste åren. Tidigare projekt som behandlar C-ITS-genomförande har granskat parternas roller, jämfört olika tekniker och granskat möjligheten att utnyttja mobilnät i genomförandet av C-ITS-tjänster. I tidigare utvecklingsprojekt har man dock inte gått in för att utarbeta en plan för införande av C-ITS-tjänster eller för att i detalj granska förutsättningarna för införande av tjänster i Finland.

Projektets mål var att granska förutsättningarna för att genomföra C-ITS-tjänster i Finland samt bereda ett förslag till nationell modell för genomförande av C-ITS-tjänster. För genomförandet av projektet ansvarade en projektgrupp, till vilken hörde Ville Kilpiö från Ramboll Oy, Jouni Rantanen och Marika Haapajärvi från Sitowise Oy samt Timo Majala, Lari Väänänen och Jarno Kallio från Nodeon Finland Oy. Projektchef för arbetet var Ville Kilpiö.

Arbetets fortskridande övervakades av en styrgrupp. Medlemmarna i styrgruppen var Risto Öörni, Mikko Räsänen, Anna Schirokoff, Pekka Pussinen, Ari Kallio och Petri Aarni från Transport- och kommunikationsverket Traficom, Petri Antola och Jari Myllärinen från Trafikledsverket, Olli Rossi och Mika Ahvenainen från Trafikstyrningsbolaget Fintraffic Väg Ab, Antti Paasilehto från Kommunikationsministeriet, Mika Kulmala från Tammerfors stad och Niko Kynsijärvi från Helsingfors stad. Ordförande för styrgruppen var Risto Öörni. Styrgruppens medlemmar bidrog till genomförandet av arbetet genom att dela med sig av sin sakkunskap till rapportförfattarna under arbetets gång samt genom att delta i kvalitetssäkringen genom att kommentera slutrapporten om arbetet.

Synpunkterna i slutrapporten är skribenternas egna och de representerar inte nödvändigtvis synpunkterna hos den myndighet som publicerar rapporten eller de aktörer som är representerade i styrgruppen.

Arbetet var en del av det europeiska projektet C-Roads Extended, som fick finansieringsstöd från programmet Ett sammanlänkat Europa (CEF, Connecting Europe Facility) 2024–2027.

Den ursprungliga rapporten skrevs på finska och översattes till engelska.

Helsingfors, den 6 juni 2025

Risto Öörni
Specialsakkunnig
Transport- och kommunikationsverket Traficom

Table of Contents

Abbreviations and glossary

3GPP	Third Generation Partnership Project, an organisation consisting of standard development organisations and industry partners dedicated to advancing technologies based on mobile network technologies.
AA	Authorization Authority, that enables authorising C-ITS stations to provide certain C-ITS services in C-ITS systems within the C-ITS Security Credential Management System (EU CCMS).
AMQP	Advanced Message Queuing Protocol that supports high data scalability and reliability between back-end systems.
API	Application Programming Interface enabled by hardware and software communications.
AT	Authorization Ticket to be handed over to C-ITS stations.
BI	Basic Interface, a protocol intended for standardised data exchange between back-end systems in long-range communication.
CAM	A Cooperative Awareness Message is a C-ITS message containing position, direction and speed data on vehicles.
CCAM	Cooperative Connected Automated Mobility.
CCMS	C-ITS Security Credential Management System.
C-ITS	Cooperative Intelligent Transport Systems, intelligent transport services provided via interactive intelligent transport systems.
C-ITS Actor	Organisations and persons involved in the operation of the C-ITS whose roles and responsibilities are defined in ISO Standard 17427-1.
C-V2X	Cellular Vehicle-to-Everythingcommunication methods developed by the 3GPP organisation for mobile network technology used in ITS communication.
CPA	Certificate Policy Authority for C-ITS.
CPOC	C-ITS Point of Contact according to the EU CCMS.
CPS	Certificate Practise Statement required from the Signing Certification Authorities in the EU CCMS.
CSMS	Cyber Security Management System
DATEX2	The European standard for the data exchange between traffic management systems and service providers (DATa EXchange).

DDoS Distributed Denial-Of-Service on an Internet network.

DENM Decentralized Environmental Notification Message, a C-ITS message that provides information on the state of traffic and the road network and disruptions.

DfRS Data for Road Safety, a European ecosystem that promotes the utilisation of SRTI data.

DNS Domain Name System, an Internet-based name service system that maintains information about the IP addresses and associated names located online.

EA Enrolment Authority, which enables the enrolment of C-ITS stations into a C-ITS service implementation in accordance with the EU CCMS.

EAL Evaluation Assurance Level, a classification of the information security of an IT system or product in accordance with ISO 15408.

ECTL European Certificate Trust List, a list of trusted PKI certificates in accordance with the EU CCMS.

EDPB European Data Protection Board.

ETSI European Telecommunications Standardisation Organisation.

EU Root CA EU Root Certificate Authority in accordance with the EU CCMS.

GDPR EU General Data Protection Regulation.

HSM Hardware Secure Module, a physical device used for the safe storage and use of encryption keys in applications requiring data security, e.g., C-ITS stations.

IEC International Electrotechnical Commission.

IEEE Institute of Electrical Engineers, an international organisation that published the IEEE 802.11 Ethernet standard, for example.

IETF Internet Engineering Task Force, an organisation responsible for the standardisation of Internet protocols.

II Improved Interface, a protocol for data exchange between interchange servers in the C-ITS systems.

IP Internet Protocol used in packet-switched networks to enable communication between networked devices.

ISMS	Information Security Management System.
ISO	International Organisation for Standardisation.
ISO 27001	An information security standard published and maintained by the ISO standardisation organisation that sets requirements for the organisation’s information security management system.
ITS-G5	Name used in Europe for short-range communication based on radio technology and IEEE 802.11 series of wireless standards used in the C-ITS system.
JRC	Joint Research Centre of the European Union located in Ispra, Italy.
NAP	National Access Point for storing relevant digital mobility data for the providers and developers of mobility services.
NIS	Directive of the European Union on cybersecurity in Network and Information Systems.
OASIS	Organisation for the Advancement of Structured Information Sharing, which consists of industry and public sector operators and research organisations and which developed and published the AMQP protocol.
OBU	On-Board Unit (C-ITS).
OSI Model	Open Systems Interconnection reference model standardised by the ITU-T standardisation organisation that describes the operation of communication connections on seven different layers.
PKI	Public Key Infrastructure, a method for the secure transfer of information in information technology.
PP	Protection Profile, a secure profile of the C-ITS station, which defines the scope of the information security evaluation according to ISO 15408.
Quadtree	Data structure commonly used in spatial data systems.
RCA	Root Certificate Authority in accordance with the EU CCMS.
RTTI	Real-Time Traffic information regulated by the European Commission Delegated Regulation 2022/670.
SaaS	Software as a Service.
SLA	Service Level Agreement.
SOG-IS	Senior Officials Group on Information Systems Security.
SPAT	Signal Phase and Timing, a C-ITS message that submits traffic light status information.

SREM	Signal Request Extension Message, a C-ITS message used to request priority at a traffic signal.
SRTI	Safety-Related Traffic Information, general minimum traffic information related to traffic safety. The data content is defined in the European Commission Delegated Regulation 886/2013.
SSEM	Signal request Status Extension Message.
SSP	Service Specific Permissions.
RSU	C-ITS Road-Side Unit.
TCP/IP	Transport Control Protocol/Internet Protocol, a combination of two protocols commonly used for communication over the Internet, where the IP protocol identifies devices, and the TCP manages connections using port numbers.
TIA	Transfer Impact Assessment, a method in line with the GDPR related to the transfer of personal data outside the EU or EEA for assessing transfer effects and the level of data protection in the target country.
TLM	Trust List Manager is an operator in accordance with the EU CCMS that manages the list of qualified RCAs and root certificates.
TLS	Transport Layer Security, a cryptographic protocol used to verify message integrity and authenticate users on the Internet.
TOE	Target Of Evaluation, the definition of the scope of the assessment of the level of information security of an IT system or product in accordance with ISO 15408.
UN R155	UN Regulation No. 155 on the cybersecurity of vehicles prepared by the UNECE, which entered into force in 2021.
UNECE	The United Nations Economic Commission for Europe.
X.509	A cryptographic standard published by the ITU-T standardisation organisation for public key encryption certificates.

1 Introduction

1.1 Background and objectives

In Finland, intelligent transport services have been developed and tested by road transport authorities both nationally and in cooperation with other countries for several years. C-ITS (Cooperative Intelligent Transport Systems) services refer to intelligent transport system (ITS) services that are implemented interactively between different systems by exchanging standardised real-time C-ITS messages, whose reliability is guaranteed through the EU's C-ITS Security Credential Management System (EU CCMS). The messages can be shared between vehicles, infrastructure and other road users. C-ITS services can be implemented through long-range or short-range communications. The C-Roads Platform, a cooperation group between European Member States and road operators, has defined implementation based on short-range communication to radio networks (ITS-G5) and long-range communication to IP networks. An implementation that supports both short- and long-range communication is called hybrid communication.

In the implementation of C-ITS services, Finland has committed to complying with the existing C-ITS standards and the definitions of the C-Roads Platform cooperation group. An important part of the national implementation model is a communication solution that serves as its basis, as the systems used for short-range and long-range communication differ in many respects. However, the two models have in common the requirements of the EU's C-ITS security and certification policies. Finland and the other Nordic countries have particularly focused on using the mobile network as a communication solution for C-ITS systems. Related research and development work has been carried out between countries, including in the NordicWay project supported by the European Commission.

The aim of the Finnish authorities is to create preconditions for the deployment of C-ITS services. However, there is currently no actual binding legislation in force on the implementation, management or administration of C-ITS services. In the past, the European Commission and the Member States have prepared and published a proposal for a regulation on interactive ITS services, which, however, was not enforced. However, there is extensive regulation and standardisation related to the organisation of C-ITS services, concerning aspects such as the structure and profiles of messages, the roles and responsibilities of operators, C-ITS stations and the EU CCMS as well as cybersecurity and data protection.

In the period 2023–2024, Finland implemented C-ITS projects that examined the roles of the parties, compared different communication technologies and assessed the capabilities of mobile networks in the implementation of C-ITS services. However, the projects did not aim to provide a more detailed description of the national implementation model or include concrete measures. The aim of this study was to prepare an implementation model for the architecture of C-ITS services in Finland and to create preconditions for the deployment of C-ITS services, taking into account the requirements set by the EU's C-ITS security and certificate policies and the national intent.

1.2 Limitations

The assessment of the socio-economic aspects of C-ITS services and the suitability of different communication technologies for the provision of services were excluded from the examination of this work.

The report does not comment on the social economic factors of C-ITS services

This study identified costs related to the deployment of C-ITS services, including the requirements of the EU's C-ITS security and certification policies. These costs are discussed in more detail in section 5.7, according to which they consist of the following areas:

- the deployment and operational management of the national central C-ITS station and interchange server
- root certificate service, establishment of a centralised national root certificate service and use of certificate services
- costs incurred by C-ITS station operators in connection with security and certificate policy requirements.

The implementation of C-ITS services also causes other costs, which may be related to, for example, the production of source data required by the services or the provision of services to end users. This report does not assess the magnitude of the costs or their distribution between different actors. The report also does not assess the impacts of C-ITS services and thus their socio-economic profitability in Finland, which is the general starting point for investments financed with public funding. To be able to recommend the implementation and deployment of C-ITS services without reservation, a more detailed cost-benefit analysis would be required. While this study included no such analysis, it is a recommended topic for further research. In connection with the need and prioritisation of C-ITS services, a separate project has been put out to tender at the time of writing this report. The key objectives of the project are to produce information on the needs of users and society related to C-ITS services, to prepare a proposal for C-ITS services to be implemented in Finland in the first phase and to prioritise the services in relation to each other (Traficom 2024). These results were not yet available at the time of completion of this report.

The report does not comment on the suitability of different communication technologies for the provision of individual C-ITS services

This report does not examine the suitability of different telecommunication technologies for the implementation of C-ITS services. Section 6.2 provides a general description of the communication technologies used to transmit C-ITS messages and discusses the technologies identified by the C-Roads cooperation platform (short-range and long-range communication and hybrid solutions) at a general level. The real focus of this report is on the areas in which the EU C-ITS security credential management system is in place. As a result, it leaves a certain degree of freedom in relation to the whole service chain implementation model, for example, for road operators to produce data and for service providers to communicate information to end users. As the study focused on providing a description of the implementation based on long-range communication, no actual comparison between short-range and long-range implementations was carried out. Instead, differences are highlighted in the report as necessary. However, there may be grounds for carrying out such a review, as further explained in Chapter 0. More generally, the capability of different communication technologies in the implementation of C-ITS services has been explored in separate studies (see, for example, Kilpiö et al. 2024 and Kynsijärvi et al. 2024).

2 Methods

The research methods included a literature review, cooperation in a steering group, expert interviews and workshops. Valuable contributions also came from consultants, relevant agencies, and the steering group members’ own expertise.

The literature review was based in particular on the C-ITS security and certificate policy documents published by the Joint Research Centre (JRC) of the European Union and the definitions published by the C-Roads Platform. The study also made extensive use of previous studies and analyses on C-ITS development and introduction.

Expert interviews were also used as an important research method that allowed exploring the interoperability of the solutions offered by commercial operators in several countries with the European C-ITS policy. The perspectives of public sector operators who have decided to invest in C-ITS development themselves were also examined.

During the work, one workshop was organised with representatives of national stakeholders to seek perspectives on the national strategic intent to promote the C-ITS implementation and to assess the functionality of different options for realising the architecture components of the C-ITS service implementation.

During the study, the steering group met four times. The steering group had representatives from the central government and the municipal sector relevant from the perspective of C-ITS development. The most important task of the steering group was to monitor and guide the progress of the work.

3 EU C-ITS security and certificate policies

3.1 Background

The EU's common C-ITS security and certificate policies were originally created in the period 2014–2017 as part of the work of the C-ITS Deployment Platform and C-ITS Platform established by the European Commission. More broadly, the work organised by the platforms and the Commission aimed to promote the deployment of C-ITS services by creating common principles for the deployment of cross-border C-ITS in Europe with key European stakeholders. The final report of the C-ITS Deployment Platform played an important role in the 2016 European strategy on Cooperative Intelligent Transport Systems (EU C/2016/766) towards cooperative, connected and automated mobility. As a result of the definition and planning of the C-ITS platforms, the first security and certificate policies for C-ITS services were published in 2017.

The objective of the C-ITS security and certificate policies are to ensure the information security of communications between C-ITS stations, such as the confidentiality and integrity of messages and the secure management of the units and the data processed by them. The security of communications is based on the public key infrastructure (PKI) method defined in the C-ITS certificate policy and the European C-ITS Trust model. The secure management of C-ITS stations is ensured by the management requirements set out in the security policy. These requirements and principles form the EU’s common security and certificate policy for C-ITS services.

The following versions of the security and certificate policies (2.0) were presented as part of the Commission Delegated Regulation proposal on the C-ITS in 2019 (EU C/2019/1789). Although the actual proposal for a Delegated Regulation was not adopted in the final vote of the Council of the European Union, all relevant stakeholders had already adopted the principles of the C-ITS security and certification policies before the publication of the proposed (EU C/2019/1789, 13). With this separate approval, the European Commission started to promote the deployment of C-ITS services in accordance with the principles of the C-ITS security and certificate policies. The activities focused in particular on the preparation of key elements of the EU CCMS and the implementation of the EU Root Certificate Authority (EU Root CA) established for piloting purposes.

A tendering process for the provision of the root verification service administered by the EU was organised in spring 2019 (JRC/IPR/2019/OP/0365). IDnomic, a French company focused on digital identity management services, was the winner of the competitive tendering process. As early as before the conclusion of the actual agreement at the end of 2019, the ownership of IDnomic was transferred to Atos SE due to a corporate acquisition, which continues to provide the service today. At the time of writing this report, the option years of the agreement were used. In accordance with the agreement, the service will be continued annually after 2022 until the end of 2026 at a maximum.

Following the work of the C-ITS forums, the C-ITS security and certificate policies has been developed by the European Commission under the leadership of the Joint Research Centre (JRC) in Ispra, Italy. The task of the JRC is to provide independent scientific and technical support to back up decision-making and policy development in the European Union. The JRC has been working in cooperation with the C-ITS Working Group (E01941) established in 2020 by the Commission’s ITS Committee (C39400), which also provides final approval to the new versions of the C-ITS security and certificate policies before they are published.

The latest approved version (3.0) of the C-ITS certificate policy, published by the EU Technical Research Centre, was released in May 2024. The latest approved version (3.0) of the security policy was released in September 2023. Both documents have been significantly updated compared to the previous versions prepared for the 2019 C-ITS Delegated Regulation proposal, although efforts have been made to maintain the basic structure of the documents.

The deployment of C-ITS services in accordance with the security and certificate policies is currently being prepared by the C-Roads Platform, a joint EU-national cooperation forum for the harmonisation and deployment of C-ITS services. The Security Aspects sub-group of the WG2 (TF 1, Technical Aspects) is specifically responsible for topics related to the security credential management system in the cooperation platform.

EU-managed systems for the distribution and management of security credentials under the C-ITS security and certificate policies have been ready for practical pilots and demonstrations since 2020 (distribution and management of so-called L0 credentials). Registration for security credentials intended for use in final C-ITS production environments (so-called L1 and L2 credentials) has been possible since December 2024. In addition to the EU root certificate service established by the European Commission and operated by ATOS, security credentials are currently distributed by some private sector actors. The operation of the L0 level credentials has been tested in Finland as part of research and analysis carried out by Traficom in 2023, “Piloting cybersecure and interoperable cellular C-ITS services” (Kynsijärvi et al. 2024).

The requirements for the use of the European Union C-ITS Security Credential Management System (EU CCMS) under the C-ITS certificate policy are regulated in the ITS Directive, which was updated in 2023. The Directive confirms the roles of the European Commission in the operation of the management system and the requirements for its use as part of the implementation of ITS services for collaborative, connected and automated mobility. (EU 2023/2661 2023)

3.2 C-ITS Certificate Policy

The C-ITS certificate policy defines the European C-ITS Trust model. The model is based on the public key method and is used as part of the EU C-ITS Security Credential Management System (EU CCMS). The Certificate Policy binds all actors joining the C-ITS system. (C-ITS Certificate Policy 2024, 11)

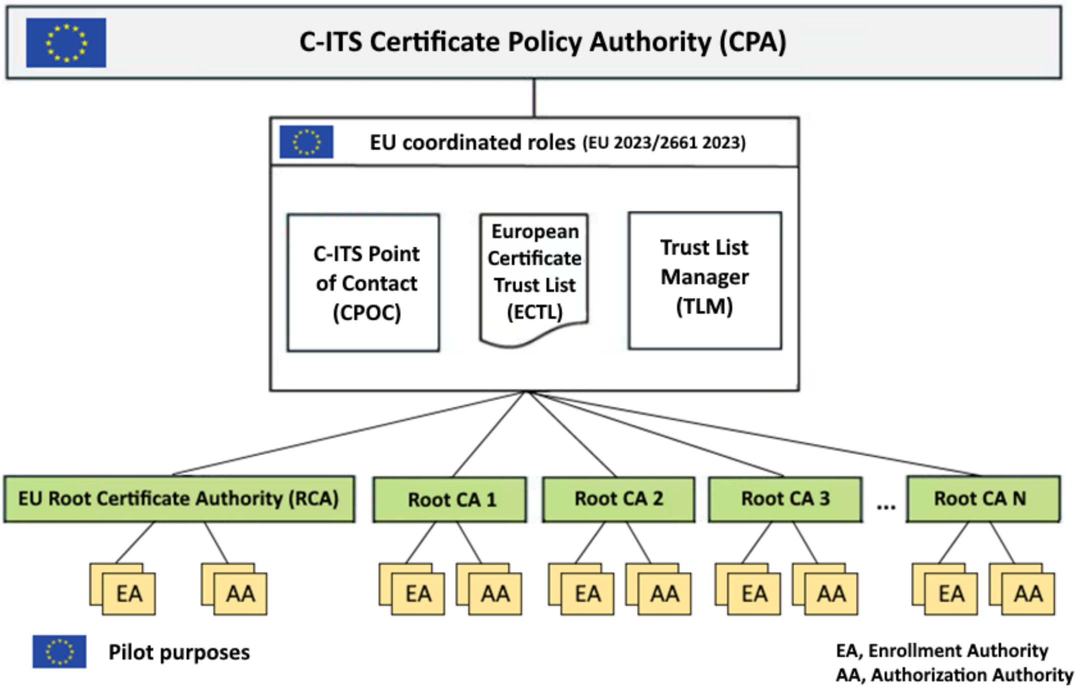

C-ITS Certificate Policy Authority (CPA)
EU coordinated roles (EU 2023/2661 2023)
C-ITS Point of Contact (CPOC)
European Certificate Trust List (ECTL)
Trust List Manager (TLM)
EU Root Certificate Authority (RCA)
Root CA 1
Root CA 2
Root CA 3
...
Root CA N
EA
AA
Pilot purposes
EA, Enrollment Authority
AA, Authorization Authority

Figure 1. C-ITS Security Certificate Management System architecture (adapted from C-ITS Certificate Policy 2024, 15)

The roles coordinated by the EU shown in Figure 1 and related responsibilities are described in Section 1.3 on the C-ITS Certificate Policy (C-ITS Certificate Policy 2024, 14–20).

The **C-ITS Certificate Policy Authority** (CPA), which operates under the direct authority of the European Commission, is the most important operator in accordance with the Certificate Policy. This authority is responsible for the overall management of the certificate policy and PKI authorisations, i.e. granting authorisations to operate as a C-ITS Point of Contact (CPOC), manage a European Certificate Trust List (ECTL) as a Trust List Administrator and serve as a Root Certification Authority (RCA). The C-ITS Certificate Policy Authority informs the party managing the ECTL of approved/non-approved RCAs.

A **Trust List Manager** (TLM) is an individual entity appointed by the C-ITS Certification Policy Authority and is responsible for managing the European Certificate Trust List (ECTL) and reports regularly to the Certificate Policy Authority on its own activities. The ECTL contains all Root Certification Authorities and root certificates approved by the CPA. The list allows all PKI parties to trust the approved Root Certification Authorities. The TLM maintains the ECTL of Certification Authorities based on C-ITS Policy Authority notifications (approved/rejected RCAs), receives root certificates from the CPOC and forwards the regularly and timely signed ECTL to the CPOC and RCAs. An Accredited PKI Auditor of the EU CCMS regularly audits the performance of the TLM.

The **C-ITS Point of Contact** (CPOC), is an individual entity appointed by the C-ITS Certification Policy Authority. The CPOC communicates with other C-ITS Trust Model parties (CPA, TLM and RCAs) in accordance with the C-ITS Point of Contact (CPOC) Protocol, whose latest version (3.0) was published in January 2024. In accordance with the protocol, after the approval of the RCA on authority by the CPA, the CPOC receives the root certificate and forwards it to the ECTL. The CPOC is also responsible for publishing the approved and signed ECTL for everyone to use.

In line with the reformed ITS Directive, the European Commission manages all three roles of the C-ITS Security Credential Management System described above (EU 2023/2661 2023). These roles can be described as the **administrative level** of the EU CCMS and the provider of centralised services. These functions provide an administrative framework for the EU's centralised security credential management system, allowing the decentralisation of the EU CCMS operations between a wide range of RCAs that can be freely cross-used by Enrollment Authorities (EA) and Authorisation Authority (AAs) at the C-ITS stations while allowing the C-ITS stations to reliably communicate between each other on a "common root of trust".

Below the centralised services of the EU CCMS (Figure 1) is the **operational level** of the management system, where a set of equal-value Root Certification Authorities (Root-CAs) authorised by the C-ITS Certification Policy Authority, together with Sub-Certification Authorities (Sub-CAs) form a mutual trust relationship. With the help of certification authorities, C-ITS stations are registered and authorised as part of the secure European C-ITS Trust model. The operations of the certification authorities are defined in the ETSI ITS communications security architecture standard (ETSI TS 102 940 2022, 42-44) and in the C-ITS Certificate Policy.

The **Root Certification Authority** (RCA) may be a commercial operator, organisation, national or European organisation. The RCA applies for authorization from the CPA in accordance with the ETSI TS 102 042 standard. When applying for authorization, the RCA must provide the information required for registering and identifying the organisation, the certification authority's digital fingerprint (root certificate's SHA-256 summary value, "hash value"), cryptographic information on the root certificate (algorithm, key lengths) and describe the **certification practices to be followed** in the management of digital certificates. The certification practices to be described include the issuance, revocation and renewal of certificates and security measures to protect the CA infrastructure (Certificate Practice Statement, CPS).

In accordance with the CPOC protocol, the information described above is physically transmitted to the European Commission's Technical Research Centre (JRC) in Italy (Ispra). After the approval step described above has been successfully completed, the RCA sends its own public certificate to the C-ITS Point of Contact (CPOC), which adds it to the ECTL. The CPOC publishes a list of TLM Certificates, which can be viewed on a website maintained by the C-ITS Point of Contact (https://cpoc.jrc.ec.europa.eu/TLMCertificates.html). An updated list is typically published every three months, and more often if necessary.

In accordance with the C-ITS Certificate Policy, two separate certification authorities operate under each Root Certification Authority: C-ITS station **Enrolment Authority (EA)** and **Authorization Authority (AA)**. The EA and AA of the C-ITS stations serve as Sub-Certification Authorities (Sub-CAs) of the Root Certification Authority (Root-CAs), and like the Root-CA, they may be commercial operators, non-governmental organisations, or national or European organisations.

Applying for authorization of a Sub-CA (certification) is a very similar process as for Root-CA. The difference is that while a Root-CA applies for authorization from the Certificate Policy Authority, the Sub-CAs apply for authorization from the Root-CA under whose authority the certification activities take place. The Sub-CA sends to the Root-CA the information needed for registering and identifying the organisation, a digital fingerprint and a Certificate Practice Statement (CPS).

In addition to the requirements described above, each certification authority (root CA, EA, AA) must attach to the authorization application the auditing report by an EU CCMS PKI auditor.

A **PKI auditor** is a member of the EU CCMS that audits the activities of the certification authorities (root CA, EA, AA) and the Trusted List Manager (TLM). The role and operating methods of the PKI auditor are described in Chapter 8 of the C-ITS Certificate Policy (C-ITS Certificate Policy 2024, 80–81).

The operations of certification authorities are audited for the first time when the authority applies for authorization and regularly thereafter at least every three years. The operator to be audited must request a new audit of the operations if there are any changes to their Certificate Practice Statement (CPS). The C-ITS Certificate Policy Authority may request a separate audit for all operators if there are significant changes to security policy. The schedule for changes to operations and audits is determined on the basis of the criticality of the changes.

An audit request to the Trusted List Manager (TLM) is made by the C-ITS Certificate Policy Authority. The Root Certification Authorities make audit requests related to their operations. In the audit, the PKI auditor focuses particularly on ensuring compliance with the C-ITS Certificate Policy, the operator’s Certificate Practice Statement (CPS) and compliance with the ISO/IEC 27001 standard for information security management. In practice, the audit can be performed by any independent entity accredited and certified by a member of the European Co-operation for Accreditation.

3.3 C-ITS Security Policy

The C-ITS Security Policy, together with the C-ITS Certificate Policy, lays the foundation for the deployment of secure and interoperable C-ITS services in Europe.

The C-ITS Certificate Policy outlined in the previous section focuses on ensuring the information security of communication between C-ITS stations. Here, the security architecture to be commonly introduced in Europe based on the Public Key Infrastructure (PKI) and the EU CCMS play a key role.

The C-ITS Security Policy is particularly focused on setting a framework and laying a foundation for information security management related to the deployment and operational management of C-ITS systems. It sets requirements related to information security management, especially for parties operating C-ITS stations and other stakeholders related to the operation. Another essential element is the requirements related to the management of the data processed by C-ITS stations. (C-ITS Security Policy 2023, 2)

In relation to the management of information security in organisations, the Security Policy requires a certified Information Security Management System from organisations operating C-ITS stations. Depending on the role of the operator, different management system requirements have been set for different operators (e.g. parties operating essential transport services, the vehicle industry, other operators involved in operating C-ITS stations). (C-ITS Security Policy 2023, 3)

Another essential element of the C-ITS Security Policy is the requirements related to the management of the data processed by C-ITS stations. The information must be managed from the perspective of potential information security threats and potential information security breaches. Threats are addressed with regard to traditional data security features, confidentiality, integrity and availability of data, and from the perspective of the severity and impact of related data breaches. The impacts of data breaches to be taken into account include examining aspects related to traffic safety, smooth traffic flow, economic impacts and privacy protection. (C-ITS Security Policy 2023, 3–5)

In addition to the management and classification requirements for data processed by C-ITS stations, C-ITS security policy sets minimum requirements for risk management. These include risk assessment practices, such as risk identification, analysis and treatment, which are discussed in Section 2.3 of the C-ITS Security Policy. (C-ITS Security Policy 2023, 5–10)

The requirements and specifications of the C-ITS Security Policy for C-ITS stations, their operations and the data processed are described in more detail in the following Chapter 4.

4 C-ITS stations and their operational management

C-ITS stations are a set of hardware and software components used to transmit and receive C-ITS messages. The reference architecture of C-ITS stations is defined in ETSI EN 302 665. The standard is particularly focused on defining the reference architecture for communication between different types of C-ITS stations (ITSC, ITS Communications). The standard defines C-ITS stations in four different types. C-ITS station types are vehicle ITS station, roadside ITS station, central ITS station and personal ITS station. Organisations managing C-ITS stations are referred to as C-ITS station operators.

The harmonised technical operation, cybersecurity requirements and requirements related to the operation of S-ITS stations are regulated by a number of standards and EU requirements. The requirements also vary depending on the type of C-ITS stations. This chapter describes the requirements related to the manufacture, information security and operational management of C-ITS stations.

The C-ITS security and certificate policies define the EU C-ITS Security Credential Management System (EU CCMS), which includes three levels of readiness (L0, L1, L2) from the testing phase of C-ITS systems (Level L0) towards a fully compliant production operation system (Level L2). For the purposes of this chapter, requirements relating to C-ITS stations and their operation comply with the final, L2 level, unless otherwise stated. Subsection 4.2.4 describes the mitigations related to L2 level requirements during operation in the L1 transitional level.

4.1 Manufacture of C-ITS stations

4.1.1 Background

The manufacture of C-ITS stations refers to the manufacture of physical devices and related software. Some C-ITS stations can only be software (e.g. central C-ITS station). The following sections describe requirements based on ETSI and ISO standards, EU directives and C-Roads Platform specifications for the manufacture of C-ITS stations.

Manufacturing requirements must naturally be taken into account as part of the production of C-ITS stations (e.g. software development of the central C-ITS station), but also as part of their procurement so that the correct C-ITS station approvals and certificates can be required in connection with the procurement.

4.1.2 ETSI standards and interoperability testing

C-ITS stations (including central C-ITS stations) and systems of PKI key suppliers must operate in accordance with the ETSI TS 102 941 and ETSI TS 103 097 standards (latest versions v.2.2.1 and v.2.1.1). The standards define the trust and privacy management of communication between C-ITS stations and the secure data structures of messages.

The interoperability tests defined in ETSI TS 103 600 aim to ensure the compliance and mutual interoperability of C-ITS stations. The ETSI standardisation organisation organises annual interoperability testing events for C-ITS station manufacturers and root certification service providers (“ETSI Plugtest™”). The testing events have a duration of around one week and involve working on test cases related to inter-device communication with the aim of ensuring interoperability between the solutions implemented by participants.

The ETSI Centre for Testing and Interoperability (CTI) organises the annual interoperability testing events described above, in which all willing hardware and software manufacturers and other organisations are free to participate to test the interoperability of their products between different manufacturers. This testing process for C-ITS stations is not (at least at present) a formal requirement of the European Commission in relation to the manufacture or commissioning of C-ITS stations, but rather a process that allows extensive testing of interoperability together with other device manufacturers. Participation in the tests typically requires the signing of a non-disclosure agreement (non-disclosure obligation related to other equipment manufacturers' products and their operations) and participants receive a certificate of participation. ETSI's Technical Committees also use these events to develop standards through feedback from hardware and software manufacturers.

4.1.3 ISO 15408 – Common Criteria

EU C-ITS Security Policy defines that the level of information security of C-ITS stations must be assessed in accordance with the ISO/IEC 15408 standard (so-called "Common Criteria"). The standard consists of five parts and the latest version (fourth edition) was published in August 2022.

ISO 15408 has been developed specifically to assess the level of information security of IT products and to ensure that the level of information security of the product meets the needs of customers (risk owner). The products can include a wide range of hardware, firmware or software. (ISO/IEC 15408-1 2022)

The certification process for the information security of a C-ITS station is a two-step process:

(1) **Definition and certification of the Protection Profile (PP) of a C-ITS station.** The first phase involves defining the Target of Evaluation (TOE), i.e. the scope of the evaluation of the information security level of the C-ITS station. This is done by means of a so-called Protection Profile (PP). The PP and related documents are certified by an approved audit organisation. (C-ITS Security Policy 2023, 9)

Defining the Target Of Evaluation and Protection Profile is essential because the standard is flexible and does not, as a rule, take a stand on whether the Information Technology Security Evaluation is carried out on a whole product or only on part of it.

(2) **Certification of the level of information security of a C-ITS station** to the extent defined by the Protection Profile**.** The C-ITS Security Policy (Section 27) defines that the information security of the C-ITS station must be assessed and certified in accordance with the Evaluation Assurance Level (EAL) defined by the ISO 15408 standard (C-ITS Security Policy 2023, 9). The C-ITS Certificate Policy (Section 323) specifies that the evaluation of the level of information security must result in the achievement of at least an evaluation assurance level EAL4 (C-ITS Certificate Policy 2024, 74) in

accordance with the used level classification. The standard contains security levels EAL1-EAL7.

According to the description in ISO 15408, EAL4 requires good development practices that are stringent but do not require significant specific competence, skills or resources. The level is applicable in situations where developers are required to have a reasonable or high level of competence related to information security management and an independent ability to ensure security in the normal production and development of commercial software. (ISO/IEC 15408-1 2022)

In practice, defining Protection Profiles (PPs), i.e. determining the required level of information security, is the responsibility of the so-called risk owner. In Europe, information security in the C-ITS system is the responsibility of the C-ITS Certificate Policy Authority (CPA), i.e. the European Commission. The C-ITS CPA creates ready-made security profiles for different types of C-ITS stations to ensure sufficient scope for the evaluation of the level of information security of the stations. C-ITS station manufacturers are obliged to use these security profiles to assess the level of information security. Approved PPs of C-ITS stations are published in the same place as security and certificate policy documents.

The C-ITS certificate policy authority has created ready-made PPs for roadside and vehicle C-ITS stations. For these stations, the PP defines that the evaluation of the level of information security must particularly target the Hardware Secure Module (HSM) of the C-ITS station, which protects the PKI keys stored in the device and the C-ITS station firmware (C-ITS Certificate Policy 2024, 74).

In accordance with the C-ITS Certificate Policy (paragraph 25), when developing new C-ITS stations, the C-ITS Certificate Policy Authority will need to define the Protection Profiles suitable for new C-ITS stations. If a PP has not yet been implemented for the C-ITS station to be deployed, the manufacturer of the C-ITS station may define the PP, and the protection level of the C-ITS station can be evaluated after approval of the PP by the C-ITS Certificate Policy Authority. In this case, a lower level of information security, EAL2, is the required level of evaluation. (C-ITS Security Policy 2023, 9)

The above should be taken into account as a part of the possible deployment of a Finnish C-ITS system, which, if based on long-range communication, would in practice only include software-based central C-ITS stations. The Certificate Policy Authority has not specified the PP required for determining the Evaluation Assurance Level of such central stations.

If the aim is to obtain an Information Technology Security Evaluation in accordance with ISO 15408 for a central C-ITS station manufactured in Finland, the Evaluation Assurance Level can be assessed by a Finnish evaluation unit approved by FINAS (Finnish Accreditation Services). However, no FINAS-approved operators specialised in the area of intelligent mobility or traffic in general have been identified in Finland. In this case, the certification may be carried out by a European evaluation unit identified in the framework of the Special Officials Group on Information Systems Security (SOG-IS) carrying out evaluations valid across Europe in line with the Mutual Recognition Agreement (MRA) principles.

4.1.4 EU Radio Equipment Directive

In addition to the information security management requirements for the products described above, C-ITS stations using radio technologies (vehicle C-ITS stations, roadside C-ITS stations and personal C-ITS stations) are also subject to Delegated Regulation (EU) 2022/30 under the Radio Equipment Directive. In particular, the Delegated Regulation applies to radio equipment that can communicate over the Internet either directly or via another device ("internet-connected radio equipment"). The Regulation contains requirements related to the use of radio network resources, network disruptions and the protection of personal data (Kotilainen et al. 2023). The date of application of the new Radio Equipment Directive has been postponed by one year from the original date (1 August 2024) to allow more time for the preparation of technical standards for information security requirements.

4.2 Operational management of C-ITS stations

The operational management of C-ITS stations refers to their responsible management. C-ITS station operators are responsible for the procurement of stations, their integration into the EU CCMS, installation, troubleshooting and information security of C-ITS stations and the data processed by them.

The C-ITS Security Policy focuses specifically on the requirements related to C-ITS stations from the perspective of their operation.

4.2.1 C-ITS Station Operator

Table 1 shows the possible C-ITS Station Operators in different C-ITS station types according to ETSI EN 302 665.

Table 1. C-ITS Station Operators by station type

C-ITS station type	Possible operators
Vehicle ITS station	Vehicle manufacturer (stations integrated in vehicles), authority (e.g. emergency vehicles), public transport operators and private service providers such as towing service providers, companies providing emergency medical transport, road maintenance contractors or volunteer fire brigade without official employment relationships.
Roadside ITS station	Road operator (State/Finnish Transport Infrastructure Agency, municipality) or other street network operator (such as a maintenance contractor whose equipment could be equipped with C-ITS short-range roadside stations).
Central ITS Station	Fintraffic (state-administered road sections), municipality (municipal road and street networks, e.g. operation of a city-specific C-ITS central station), vehicle manufacturer (central system for C-ITS in-vehicle integration in a long-range communication solution), public transport operator, other authority or private commercial operator (e.g. a C-ITS service provider that offers C-ITS services through mobile applications).
Personal ITS station	Station manufacturer (the working group is not aware of the manufacturing of personal C-ITS stations thus far).

4.2.2 *Information security management system requirements*

The information security management system requirements presented in this section are described in Section 2.1 of the C-ITS Security Policy 2023, 3.

The C-ITS Security Policy specifies that the C-ITS station operator must have an Information Security Management System (ISMS) certified in accordance with ISO/IEC 27001. The Security Policy requires that, in addition to its standard requirements, the ISMS must also cover the security management of the C-ITS stations and the data they process, including data classification and the background systems that handle the data.

Alternatively, in relation to the operational management of vehicle-integrated vehicle C-ITS stations, the C-ITS station operator (typically the vehicle manufacturer) may be certified with a Cyber Security Management System

(CSMS) referred to in UN Regulation No. 155 (UN R155)[1]. To the extent that the above-mentioned CSMS does not cover the operations of the C-ITS station operator, for example, with regard to data exchange interfaces or data processing, the information security of these sections must be secured by a certified ISMS in accordance with ISO 27001.

C-ITS station operators providing essential transport services in accordance with the NIS or NIS2 Cybersecurity Directives[2] may apply the requirements of those Directives to information security management. For an operator providing a transport service, a comprehensive conformity assessment of the requirements set out in those Directives, carried out by a nationally accredited operator, is sufficient.

In addition to the certification requirements for ISMSs described above, the C-ITS Security Policy obliges C-ITS station operators to ensure that the certified security management system is consistent with the C-ITS Security Policy. This applies specifically to the requirements related to the management of data processed by C-ITS stations, which are described in Section 4.2.3 of this document.

Section 2.1 of the C-ITS Security Policy also specifies that C-ITS station operators must identify legal regulations related to C-ITS and their operation, such as the European Strategy on Cooperative Transport Systems (EU C/2016/766 2016) and the EU General Data Protection Regulation (GDPR)[3]. Station operators must also identify stakeholders related to their activities, which are an essential part of the ISMS and its requirements.

[1] The objective of the UN Regulation 155 (part of the so-called ‘E-regulations’ for the automotive industry), which entered into force in 2021 (01/2021), is to develop the cybersecurity of vehicles and is part of a wider effort to improve vehicle reliability and security in the era involving digital threats (UN Regulation No. 155, 2021). UN R155 was prepared by the United Nations Economic Commission for Europe (UNECE).

[2] The NIS2 Directive (Network and Information Security, EU 2022/2557 2022) is the second version of the European Union Cybersecurity Directive, which entered into force in October 2024. It defines the European critical operating areas for which its requirements apply (the transport sector is one of them). It defines requirements for the management of cybersecurity for organisations operating in the sector. Typically, these requirements are mostly easiest to meet by certifying an Information Security Management System in accordance with ISO/IEC 27001.

[3] GDPR (General Data Protection Regulation) is a European Union regulation aimed at harmonising data protection legislation in the European area. The Regulation became applicable on 25 May 2018. (EU 2016/679, 2016)

4.2.3 *Management of C-ITS data*

The C-ITS Security Policy defines the information management requirements related to the operational management of C-ITS stations, which must be consistent with the unit operator's ISMS. Information management requirements are (1) classification of information and associated risks, (2) risk assessment according to the classification criteria and (3) risk treatment principles.

Information classification and associated risks

Section 2.2 of the C-ITS Security Policy states that the C-ITS station operator must assess and classify threats related to the data processed by C-ITS stations, considering the security attributes of the data - confidentiality, integrity, availability - as well as the severity and impact of potential security breaches.

Table 2. Security breach assessment (C-ITS Security Policy 2023, 4)

	Potential impact		
Safety objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and confidential information.	The unauthorised disclosure of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.
Integrity Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity.	The unauthorised modification or destruction of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.

The Security Policy defines that security breaches affecting the confidentiality, integrity, or availability of messages used in the implementation of C-ITS services (CAM, DENM, IVIM, MAPEM, SPATEM, SSEM, SREM) are, by default, assumed to cause either low or moderate impact on the organisation’s operations, organisational assets, or individuals as described in Table 2 above.

The C-ITS station operator must assess the damage and costs to C-ITS stakeholders caused by security breaches from the perspective of the following impact types:

- **Safety**: the impact places road users or any of the C-ITS stakeholders at imminent risk of injury.
- **Operational impacts**: the impact is substantially negative for road traffic efficiency, or other societal impact such as environmental footprint and organised crime.
- **Financial impacts**: the impact results in direct or indirect monetary costs for one or more of the C-ITS stakeholders.
- **Privacy**: Violations of the EU's General Data Protection Regulation (GDPR) have both legal and financial impact.

Risk assessment

The C-ITS Security Policy obliges C-ITS station operators to assess the risks related to the processing of C-ITS data in a versatile manner (C-ITS Security Policy 2023, 5–7). It requires the station operator to periodically identify and assess the risks to the data processed in connection with C-ITS services. The risk assessment must be documented and include the following aspects related to risk assessment in accordance with the guidelines and requirements of ISO/IEC 27005 or ISO/SAE 21434.

- **The object of risk assessment**, including a description of the C-ITS system (purpose, scope, information handled by the system).
- Potential **impacts of data breaches** of varying levels of severity from the perspective of the impact types described above.
- **Risk identification** is based on identification and definition of the protected information (C-ITS messages and other information required for the implementation of the services) as well as the identification of potential threats and vulnerabilities related to it. Threats and vulnerabilities should be further specified through case scenarios that identify the sources of threats and the consequences of data breaches.
- **Risk analysis** examines the level (low, moderate, high) of the impact of data breaches related to risk assessment as well as the likelihood of an incident identified by case scenarios (unlikely, potential, likely). The final risk level is assessed as the outcome of the two variables as presented in Table 3.

Table 3. Determination of risk levels as the product of the likelihood and impact of potential security breaches (C-ITS Security Policy 2023, 6)

Risk levels as product of impact and likelihood		Likelihood		
		Unlikely (1)	Possible (2)	Likely (3)
Impact	Low (1)	Low (1)	Low (2)	Moderate (3)
	Moderate (2)	Low (2)	Moderate (4)	High (6)
	High (3)	Moderate (3)	High (6)	High (9)

Risks to the C-ITS service in accordance with the principles of the risk assessment described in this section and Table 3 must be handled in accordance with the following section (risk treatment).

Risk treatment

This section describes the requirements related to risk treatment in accordance with the C-ITS Security Policy. Risk treatment involves different approaches and risk management measures aimed at ensuring the confidentiality, integrity and availability of the data processed by C-ITS services.

In all cases, the **identified risks must be treated** in one of the ways described below, and their treatment procedures must be documented in accordance with the applicable standard.

- Lowering the risk level by means of risk control measures described in Sections 2.4.2 and 2.4.3 of the C-ITS Security Policy 2023 (7–9).
- Risk retention (where the level of risk meets the risk acceptance criteria).
- Risk avoidance.
- Risk sharing or transfer. However, risk sharing or transfer to mitigate risk may not be transferred to other actors in the C-ITS network in such a way as to create unacceptable residual risks.

Risk management and the related requirements are part of risk treatment. The C-ITS Security Policy defines the means of risk management mainly based on the manufacture of C-ITS stations, communication between the stations and their operation as a part of the EU CCMS. The means are mainly based on the requirements mentioned in the C-ITS Security and Certification Policies in relation to the standards applied in the operations.

Some of the above-mentioned risk management methods have already been presented in this report. Below is a compilation of all methods related to the control of data breaches under the C-ITS Security Policy.

- The methods described in the ISO/IEC 27001 or UN R155 (Appendix 5) standards must be applied to the risk management of C-ITS stations.
- To protect the privacy (confidentiality) of mobile C-ITS communications, the sender must use an Authorization Ticket (AT) change procedure for communications. The AT is used to confirm the right of the communicator to participate in the communications of certain C-ITS services (message types). They function as short-term certificates, enabling communications without revealing the actual or pseudonymised identity of the device or vehicle.
- The integrity of the data sent and received by fixed and mobile C-ITS stations is ensured by the signing of messages in accordance with ETSI TS 103 097. When operating as part of an Internet Protocol (IP) network, C-ITS stations may also use certificates based on the future ETSI ITS standard profiling ISO 21777.
- In relation to availability, it is specified that the recipient of a Signal Request Extended Message (SREM) requesting traffic light status information (moving unit) must respond to the signal with a Signal request Status Extension Message (SSEM).
- The C-ITS Security Policy highlights the following means of controlling the security risks associated with the confidentiality, integrity and availability of data processed by C-ITS entities:
    - Requirements under the ISO 15408 (Common Criteria) related to the manufacturing of C-ITS stations. These requirements are described in more detail in Section 4.1.3 of this report.
    - C-ITS stations must be interoperable with the requirements of the Certificate Policy when operating as part of the EU CCMS.
    - Controlled treatment of data breaches of C-ITS stations. In addition to the provisions of the NIS2 Directive, the stations must provide log data on incidents related to a breach for retrospective analysis.
    - The C-ITS station operator must have a certified ISMS in accordance with ISO 27001 unless it is a road operator for which a comprehensive conformity assessment of the requirements set out in the NIS1 and NIS2 Directives is sufficient. These requirements are described in more detail in Section 4.2.2 of this report.

4.2.4 Mitigations related to information security level L1

To support the deployment of C-ITS services, the EU CCMS defines three levels (L0-L2) that provide a path from the test phase to the full implementation in accordance with the C-ITS Certificate and Security Policies.

This section provides a rough description of the three-level impacts, especially for C-ITS stations and their operators. This section is based on Annex 8 to the C-ITS Point of Contact Protocol (CPOC Protocol 2024, 89–103)

The L0 level is used for the testing and competence-building towards C-ITS security standards and technical requirements conformity of C-ITS stations. L1 is a temporary environment, i.e. a transition phase for C-ITS services towards the actual L2 production environment. It should be noted that testing C-ITS stations does not, it itself, require registering them to L0. The L0 environment is intended for interoperability tests of C-ITS stations as a part of the EU CCMS. The L0 environment is offered for time-limited testing sessions (e.g. C-Roads Platform interoperability pilots) agreed upon in connection with the registration of PKI participants.

Levels L1 and L2 serve as production environments where L1 is intended for C-ITS stations that have not yet reached full compliance under the Certificate and Security Policies. The definition of L1 also includes the "L1 Legacy" track. This refers to a phase in which the L1 transition phase services have already been discontinued, but the units deployed during the transition phase will continue to operate as part of the L2 environment.

L1 is intended to support the deployment of Day 1 C-ITS services during the transition period. Based on C-Roads Platform, the transition phase is scheduled until the end of 2025 (CPOC Protocol 2024, 92). The transition period includes two years for product development and certification, after which C-ITS services in L1 production should be transferred to L2. Adhering to this schedule is unlikely as the C-ITS Point of Contact (CPOC) has only been able to register L1 and L2 level certificates for use since December 2024.

The objective of L1 is to serve as a transition phase between L0 intended for piloting and L2 intended as a permanent production phase. In relation to C-ITS stations used in C-ITS services and their operation, exceptions to the access criteria of L1 requirements have been defined in relation to L2 services. On the below eight-item list, items 1–4 apply to the security and functionality requirements related to the C-ITS stations, items 5–6 apply to exceptions related to the information security system of C-ITS station operators, and the remaining exceptions (7–8) apply to PKI operators. Table 4 below briefly describes the content of each exception.

Table 4. L1 exceptions specified in Appendix 8 of the CPOC document. A level L1 exceptions column also includes the L2 requirement after the L1 exception (CPOC Protocol 2024, 94–96)

Item	Scope	Reference	Level 1 exception	After transition phase
1	C-ITS station, CC certification	Security Policy (25)	An evaluation of the C-ITS station by a SOG-IS-recognized test lab. Protection against an attacker with basic attack potential according to EAL-level1 requirements. Addition: The L2 target level is EAL4 in accordance with the Common Criteria.	The same exception is allowed for units put into service before the end of the transition period.
2a	C-ITS station, Secure Element	Certificate Policy (324)	The manufacturer is certified according to ISO 27001. The hardware platform must achieve (in the future) Common Criteria EAL level 4 (hardware + firmware). Addition: EAL level 4 not yet required on L1, see the second part of the requirement below (2b).	The same exception is allowed for units put into service before the end of the transition period.
2b	C-ITS station, Secure Element	Certificate Policy (324)	A SOG-IS MRA accredited laboratory must send progress reports every 6 months, which the CPA assesses in order to maintain the L1 enrolment.	The same exception is allowed.
3	C-ITS station, Validation of ECTL	CPOC Protocol, Chapter I.6.2	The update of the TLM Certificate is also allowed using a secure network connection. Addition: L2: Physically in Italy.	Exception allowed
4	C-ITS station, Protocol	Certificate Policy, References to ETSI TS 102 941	Exceptions to the enrolment and authorisation of a C-ITS station may be granted if the same level of security and privacy has been certified by an accredited auditor. ETSI TS 103 097 standard certificate profiles must be adhered to.	Exception allowed

Item	Scope	Reference	Level 1 exception	After transition phase
5	C-ITS station operator, ISMS	Security Policy (1)	No ISO 27001 certification requirement. Comparable security management processes must be used. Addition: On L2, external ISO 27001 (or UN R155 or NIS1 and NIS2) certification is required.	No exceptions allowed
6	C-ITS station operator, Compliance Audit	Security Policy (31), (32), (33)	The compliance audit for the Security Policy may be conducted internally. The C-ITS station operator shall submit the resulting statement of compliance to the PKI operator. Addition: L2: External certification.	No exceptions allowed
7	PKI, Compliance Audit	Certificate Policy, Chapter 8	If there is no ISO 27001 certification, documentation describing the compliance of the information security of operations with the standard must be presented. Addition: In practice, a description of the ISMS and an internal audit report.	No exceptions allowed
8	PKI, Root CA naming convention	CPOC Protocol, Chapter 1.3.2.2	The naming convention for the CertificateID in RCA certificates as specified by the CPOC protocol is not enforced.	No exceptions allowed.

5 Deployment of the C-ITS Security Credential Management System in Finland

This chapter discusses the requirements the EU C-ITS Security Credential Management System (EU CCMS) and the related C-ITS Security and Certificate Policy requirements mandate on the deployment of the national C-ITS service architecture. It includes requirements, observations, and recommendations related to the manufacturing and procurement of C-ITS stations, the establishment of a root certificate service, joining C-ITS stations into the PKI certificate solution and the operational management of C-ITS stations.

The observations presented in this chapter are partly related to the requirements presented in the standards and the specifications of the C-ITS system (mainly the C-ITS Security and Certificate Policies and the C-ITS Point of Contact documents). The perspectives presented in the chapter are partly based on expert interviews carried out by the working group and on the viewpoints resulting from the literature review.

5.1 Procurement of C-ITS stations

The C-ITS station operator is responsible for the operational management and compliance of the stations it manages. In practice, this means that the station operator should ensure, in connection with the procurement, that the procured stations have valid information security level EAL4 certification in accordance with ISO 15408, based on the Protection Profile implemented or approved by the Commission. It could also be beneficial to request from supplier a certificate confirming their participation in an ETSI plugtest event. It should be noted that the document is not a formal demonstration of the compliance of the C-ITS station, but rather a demonstration of the work carried out by the C-ITS station manufacturer to ensure interoperability. If a C-ITS station operator procures a C-ITS station, the simplest approach is to require and verify the necessary certifications at the time of procurement.

If the C-ITS station operator decides to develop its own C-ITS station, the requirements presented in this chapter must be taken into consideration in the development.

5.2 Procurement (or development) of central C-ITS stations

One of the agreed priorities of this study was the use of long-range communication in the implementation of the C-ITS system. In light of this priority, this chapter addresses aspects related to the procurement or manufacture of central C-ITS stations, in addition to the general requirements for all C-ITS stations described in the previous chapter. Some of the perspectives highlighted are based on C-Roads Platform specifications and some on expert interviews conducted as a part of this study.

From the start, the technical development, standardisation and definition of the European C-ITS system has been very strongly based on the use of a short-range communication solution, which was also strongly reflected in the 2019 Delegated Regulation proposal (EU C/2019/1789 2019). The definition of the C-ITS system based on hybrid technology and IP-based long-range communication has been carried out in C-Roads Platform Working Group 2's (Technical Aspects) sub-group

4 (Hybrid Communication). In a separate C-ITS IP Based Interface Profile 2024, this working group has defined architectures and interfaces based on long-range communication solutions (latest version 2.1.0).

The above-mentioned C-Roads Platform specification contains a number of important definitions related to the use of long-range communication, in particular the protocols used for communication between central C-ITS stations and interchange servers[1], any networking topologies between central C-ITS stations and interchange servers, and the limits to the scope of the C-ITS trust model in an architecture based on IP networks. These principles are described in more detail in Chapters 6 and 7 of this report. Despite this work to define technical architectures that utilise central C-ITS station solutions, this technical solution still includes perspectives related to development or procurement that need to be taken into consideration.

Central C-ITS stations fully compliant with EU CCMS requirements (especially L2 requirements) that can be purchased as a finished product are not available on the market. Of course, it can be assumed that as the work on the architecture of solutions based on long-range communication makes progress in C-Roads Platform (e.g. definition of the security profile related to the central C-ITS station) and as a new Delegated Regulation on C-ITS is adopted, these will be brought to the market relatively soon. Table 5 presents the perspectives on C-ITS stations identified in the market that emerged in the expert interviews.

[1] Interchange servers are part of the C-ITS implementation based on the EU trust model. Although they do not fall within the trust domain of the EU CCMS, they act as interconnection points between national and regional C-ITS implementations, transmitting C-ITS messages between them. The operation of interchange servers has been defined by C-Roads Platform (C-ITS IP Based Interface Profile 2024), and they are discussed in Chapter 7 of this study.

Table 5. Observations related to the central C-ITS stations based on expert interviews

The product known to the working group, TLEX, developed in the Netherlands, partially supports the C-Roads Platform requirements, but not with regard to aspects such as the signing of messages between C-ITS stations. However, the supplier is willing to develop the product in accordance with the requirements set by the European Commission in the future. The product currently serves as the central C-ITS station (known as the Exchange Node in the Netherlands) of the largest European C-ITS ecosystem. (Monotch interview 2024)
Intens, a Czech company, has a central C-ITS station (Intiq) product with PKI support in accordance with the EU CCMS, which includes a wide range of central C-ITS station features. Intens recognises that the EU CCMS and C-Roads Platform specifications are still incomplete for central C-ITS stations based on long-range communication systems. Intens participates in C-Roads Platform cooperation and strives to influence its future definition work to remedy these shortcomings. (Intens interview 2024)
The Norwegian Public Roads Administration, Vegvesen, is developing a central C-ITS station. The central C-ITS station is expected to reach the first production version phase during the first half of 2025. The Norwegians are carrying out development work in a frontloaded manner even though the current requirements and C-Roads Platform specifications identify shortcomings related to the implementation method of the central C-ITS station (e.g. lack of Protection Profile, requirements for the use of HSM modules). The implementation by the Norwegians does not involve HSM modules in a data centre environment. Instead, the secure storage of PKI keys and message signatures is implemented with a program-based solution. Unlike the Norwegians' implementation of an interchange server, this implementation has not been made available as an open source platform at least during the development phase, and it is still unknown whether this will be done in the future. (Vegvesen interview 2024)

<u>Development of central C-ITS stations</u>

The perspectives outlined below should be taken into consideration if the operator intends to start developing its own central C-ITS station.

The strong emphasis on short-range communication related to the development of the technical architecture of C-ITS services is reflected in issues such as the lack of availability of the ISO 15408 Common Criteria Protection Profile (PP) related to central C-ITS stations from the European Commission. At least at the time of writing the report, the developer of a central C-ITS station must independently develop a PP defined by the scope of the determination of the Evaluation Assurance Level (EAL) for the central C-ITS station and have it approved by the Certificate Policy Authority before the actual definition of the EAL.

The specifications related to the technical architecture of the EU C-ITS services include, for the technical structure of C-ITS stations, a requirement for the use of Hardware Security Modules (HSM) as a storage location for PKI keys and for the implementation of signatures in communication between the stations. For roadside and vehicle stations, this is highlighted in the C-ITS Certificate Policy in the definition of the Protection Profiles for these stations, which include an assessment of the level of information security of HSM modules. For central C-ITS stations, no similar definition is available for a PKI key storage management solution.

Based on the expert interviews, some believe that the use of HSM security modules is currently the prevailing thinking, and as a result, HSM modules should also be used in central C-ITS stations (Teskalabs interview 2024, Microsec and Commsignia interview 2024). Some experts perceive the HSM modules as a relic of the work on defining solutions based on short-range communication, as HSM modules specifically contain significant and expensive features related to ensuring physical information security (e.g. destroying PKI keys if an attempt is made to forcibly open the HSM module). Based on the same interview, high-security data centres would serve as a natural location for central C-ITS stations, in which case such features would, in any case, be unnecessary (Vegvesen interview 2024). It was also revealed that as the matter is currently unclear as regards the C-Roads Platform specifications and the definition of the certificate and security policies, this issue will be raised for discussion in the C-Roads Platform working group (Almaviva interview 2024).

The above considerations related to the storage method of PKI keys have a significant impact on the development of central C-ITS stations, as the use of HSM modules affects the implementation architecture of central C-ITS stations and can be a significant cost item in the central stations used to transmit a significant number of messages (up to several billion per day). This may also pose scalability challenges to the central station. To clarify this issue, further definitions are currently required from C-Roads Platform (WG2 Technical Aspects→ Security Aspects). This topic is also discussed in more detail in the following Chapter 6 of this study.

The working group has also identified open software libraries available as source code that can be used in the development of central C-ITS stations on the market. One example is the Vanetza project carried out in Germany, which was originally used to develop software libraries for C-ITS implementations based on ITS-G5 short-range communication. The development work was based on the Car2X research programme aimed at improving traffic safety carried out at the CARISSMA research centre of Ingolstadt Technical University and the work of Raphael Riebl, a researcher at the university. Components developed in the project and shared openly under the LGPLv3 licence (C++) can also be utilised in IP-based solutions for long-range communication (https://www.vanetza.org/).

While the above issues do not exactly provide clear instructions for the implementation or procurement of central C-ITS stations, they highlight the development work carried out in Europe and also bring attention to the ambiguities and gaps related to the current C-ITS specifications, which particularly organisations aiming to manufacture their own central C-ITS stations as well as those looking to procure them should understand.

Chapter 7, which focuses on the C-ITS interchange servers, discusses in detail the perspectives related to developing an interchange server. The perspectives presented in this chapter are also suitable for the development of central C-ITS stations.

5.3 Organisation’s Information Security Management System

This section compiles the requirements of the C-ITS Security Policy related to the ISMS and the operational management of the C-ITS stations and highlights relevant perspectives related to this topic.

The C-ITS station operator must develop and implement an ISMS in accordance with ISO 27001. The ISMS must be certified through an external audit. The information security management system requirements vary in relation to the role of the C-ITS operator (e.g. NIS2 operator or representative of the vehicle industry). These requirements are described in more detail in Section 4.2.2 of this report.

An Information Security Management System (ISMS) is an internal development project of an organisation operating as a station operator, which is used to develop the organisation’s information security management and operational processes and tools related to information security management. The system must take into account and be consistent with the C-ITS Security Policy. This particularly applies to the requirements for the management and classification of data processed by C-ITS stations and risk management set out in the C-ITS Security Policy, which are described in Section 4.2.3.

The time spent on developing and certifying the ISMS varies considerably depending on the resources available, the commitment of management, the coverage of the management system (i.e. the entire company or only a part of it) and the initial level of information security management. On average, the certification process typically takes around 1 to 2 years from the start of the project. This assessment is based on the opinion and personal experiences of the working group on the matter.

It should be noted that it is not necessary to develop the ISMS to cover the entire organisation in accordance with the C-ITS Security Policy. It is sufficient that the system’s scope is limited to the operational management of C-ITS stations. In practice, this means the management, deployment, and maintenance of C-ITS stations, as well as the risk management of the data they process, and the risks associated with the related systems.

When establishing a national C-ITS ecosystem, it is also a good idea to consider any indirect impacts on private sector actors caused by ISMS requirements. As a rule, the requirements of the C-ITS Security Policy apply to all entities responsible for the operational management of C-ITS stations, which will mainly include road operators, i.e. states and municipalities. In practice, this means that the requirements imposed on customers will become part of the competitive tendering processes for central and local government C-ITS systems. As a result, they also apply indirectly to private sector actors that will be part of the development, management, maintenance and upkeep of C-ITS stations in the future. For customers, the direct transfer of C-ITS Security Policy requirements to suppliers is, in practice, the only way to ensure that companies operating as part of the C-ITS ecosystem meet the requirements set for customers.

The indirect transfer of requirements, originally imposed on customers to suppliers – as described above - has become evident in Finland, notably as a consequence of the adoption of the NIS2 Directive. In 2024, the requirements related to the management of information security in companies have become clearly more common in competitive tendering in the transport sector. The requirements are in line with the information security management requirements set for customers in accordance with the NIS2 Directive.

The indirect transfer of requirements will put a significant amount of pressure on the private sector related to the development of information security management. This may be reflected as problems for companies to meet the requirements and therefore an opportunity to respond to competitive tendering in the sector. The requirements also affect the cost structure of companies operating in the sector through the development of ISMS, new administrative requirements and the development of IT systems, their maintenance and regular audits.

However, the costs of ISMS for organisations are not limited solely to the development phase of the system and annual audits. An ISMS also has a cost-increasing impact on companies’ continuous operations due to a higher administrative workload related to information security (including information security, risk management teams, system maintenance and development), expenses associated with new IT systems, as well as higher information security management requirements related to project and service activities. All these changes in cost structures of companies naturally also put pressure on billing rates.

Ultimately, the increased information security requirements will enhance the security of solutions, information management, and operational security within the sector, aligning with the Commission's Europe-wide objective. However, security comes at a cost. The costs of commissioning and maintenance caused by information security management systems are assessed separately in Section 5.7.3.

5.4 PKI system root certificate service options

The C-ITS station operator must decide which EU CCMS certificate service provider it will work with to register and manage the C-ITS stations.

The EU CCMS enables the registration of C-ITS stations in the system of any certificate service provider approved by the Certificate Policy Authority (CPA). It is possible to use the EU Root Certificate Authority service maintained by the European Commission and operated by Atos, a paid version of the service provided by the same supplier or other paid root certificate service provided by private operators. Based on the ECTL list of approved L0 certificates, the most commonly used services currently include the Hungarian Microsec and Czech Teskalabs. At the time of writing, the L1 level certificates enabled at the end of 2024 were only offered by the EU Root CA maintained by the Commission itself and by Microsec (CPOC-WEB Logbook: Level 1 Environment). The final L2 level certificates had not yet been registered for use in early 2025.

Based on interviews with certificate service providers, the free EU root certificate service maintained by Atos is intended for piloting use and was not originally intended for use in large-scale final L2 production environments (Teskalabs interview 2024, Microsec and Commsignia interview 2024). The current agreement on the root certificate service maintained by the EU will continue until the end of 2026 at maximum. There is currently no information on whether the service will continue after this. Nevertheless, it is clear that in the specifications under the new ITS Directive, the European Commission does not have a formal role or responsibility to provide the service. Atos is also developing and offering a paid version of the PKI service. The technical implementation of this service and the services offered to customers will be developed further.

According to the expert interviews with private operators, service providers have an interest in developing certificate services into more extensive production environments in the future while at the same time continuously developing web portals for certificate service management and other features related to certificate management. These include certificate management API services that enable customers to develop and automatise certificate management with a program-based solution. The objective of this development is to build close partnerships with customers, which includes serving as a consultant to customers in certificate management, enabling improved customisation of certificate management and smoothness and accessibility through web portals, and possible automation related to certificate service activities, such as the use of software-based API services for certificate management. (Teskalabs interview 2024, Microsec and Commsignia interview 2024)

The interviewees also noted that their own national certificate service provider would provide better management for the large-scale and long-term enrolment of C-ITS stations than a model providing C-ITS operators with completely free access to European PKI service providers. The certificate service provider serves as a partner and expert of national authorities in relation to the enrolment activities of C-ITS stations, manages the requirements of the EU CCMS, certification processes and provides better opportunities to define national rules in relation to enrolment.

The above benefits are achieved in a situation where a single authority operating at the national level, such as a competent authority, coordinates service-specific authorisations granted to C-ITS stations, for instance. When granting service-specific authorisations, it is ensured that the applicant has, or is granted, user rights to the national root certificate service, where they are directed to register new C-ITS stations. This benefit is particularly evident in the deployment of C-ITS stations for governmental use, where the required authorisation from the competent authority can be combined with obtaining certificates from a national centralised service.

5.5 National root certificate service

This section highlights different options for implementing the root certificate service. The differences between the options are highlighted based on interviews with certificate service providers and the solutions available on the market. (Teskalabs interview 2024, Microsec and Commsignia interview 2024)

Obtaining own root certificate service is typically related to situations where the operator (C-ITS station operator or, for example, a competent authority) feels that they need a longer-term partner for the enrolment of C-ITS stations. The establishment of a national root service would be such a situation. Based on the interviews, the following options are identified for this type of situation:

(1) acquiring a shared root certificate service for several customers as a SaaS (Software as a Service) solution from a private service provider

(2) acquiring a dedicated root certificate service environment as a SaaS solution for own use only from a private service provider

(3) implementing a data centre solution under own control (on-premises) and installing a root certificate service environment intended for managing the service provider's certificates (local implementation reserved for the customer's purpose)

(4) developing your own root certificate service environment (software solution) and implementing it in your own local data centre environment (on-premises).

According to the interviewees, the easiest and most cost-effective way to purchase certificate services is as a cloud-based shared certificate service (SaaS) from a certificate service provider's environment in line with option 1. In this case, there is no need for separate certification policy authority approval and audit activities for the implementation of the root certificate service, as the operating environment used to deliver the service has already passed these requirements. (Teskalabs interview 2024, Microsec and Commsignia interview 2024)

Another method involves acquiring a dedicated certificate solution (SaaS) from a private service provider, fully independent from the certificate service activities used by other customers, in line with option 2. In this model, the service provider implements a new dedicated SaaS certificate solution in its own server or cloud service environment alongside a shared PKI solution. The implementation requires that the new certificate service is registered in the EU CCMS and passes all approval procedures that apply to certificate service providers. In practice, the service provider manages the necessary initial and periodic approvals of the dedicated certificate environment as a part of the approval procedures for their shared certificate environment. This streamlines the approval processes but still increases the administrative workload and costs related to a fully shared certificate environment.

The third method is similar to the previous solution in that it also provides the customer with access to a dedicated certificate service environment implemented for their own use. However, the difference is that the service provider does not implement in a separate server or cloud service environment, but the service is, instead, implemented in a location indicated by the customer (data centre environment owned and managed by the customer). This so-called on-premises model is even more demanding than the previous one. In this model, the certificate service environment also requires all approvals under the EU CCMS, and the approval procedures also target the physical level of the service environment, which is audited as a part of the deployment of the certificate service environment (e.g. physical separation of sub-CAs). At the same time, more of the responsibility for environmental management is transferred to the customer who is responsible for the audits of the environment. Customers are also required to have a certified information security management system in accordance with ISO 27001. While the customer can obviously use a partner for these tasks (installation, management, audits), the customer nonetheless plays a considerably more significant role in this model than in option 2 described above.

In the final, fourth model, the outcome is similar to the previous model, but the key difference being that, in addition to its own data centre service environment, the software solution for certificate management and distribution are also implemented in-house. This is naturally a long development process and requires significant special expertise from the provider in the implementation and management of PKI environments, resulting in substantially higher costs compared to the previous model.

Based on expert interviews with the root certificate service providers, in practice, national or other extensive C-ITS implementations have ended up using the option 1, 2 or 3. The different options are discussed in more detail in Section 5.7.2 of this report, which includes a comparison of the different services in terms of possible costs and benefits.

5.6 Registering a C-ITS station in the C-ITS Security Credential Management System

If a C-ITS station is not pre-registered in the EU CCMS by the station manufacturer, the C-ITS station operator is responsible for this measure.

The C-ITS station operator carries out the registration of stations in one of the ways mentioned in the previous section: using the free EU root certificate service, a private certificate service provider's shared service or a separate root certificate service implemented at the national or organisational level.

Detailed practices related to certificate management for the registration of C-ITS stations vary according to the features of the service implemented specifically to the certificate service provider and the Certificate Practise Statement (CPS) of the certificate service provider. The registration of stations may also involve a lot of nationally agreed and regulated practices. In its report, C-Roads Platform has identified that practices vary considerably between EU Member States: for example, service-specific permits may have been granted by a certificate service provider, road operator or other authority depending on the service and legislation (Kotilainen et al. 2023).

Based on interviews with certificate service providers, certificate service providers currently offer all the different parts of certificate services (root certificate and sub-certificate services), so the entire registration process can be handled with the selected individual root certificate service provider. (Teskalabs interview 2024, Microsec and Commsignia interview 2024)

The technical implementation of the registration of a C-ITS station is carried out with the help of sub-certification authorities (Enrollment Authority, EA and Authorization Authority, AA) in accordance with the C-ITS Certificate Policy. The registration request contains basic information related to the C-ITS station (quantity, purpose, activity time) and basic information about the registration organisation (unique identifier, contact details, contact persons). As part of the registration process, the certification authority is provided with information and any national authorisations on the C-ITS services used, based on which the registration authority issues service-specific permits (SSP) to the C-ITS station. At the same time, a PKI key pair is created, which is stored in the C-ITS station in addition to service-specific authorisations. The PKI keys enable the station to join the EU's C-ITS service implementation architecture and implement C-ITS services in accordance with service-specific permits. The methods of implementing the process vary between the root certificate service providers, depending on the certificate provider’s own process and the method of implementing the service offered for registration.

Based on a pilot project previously carried out in Finland (Kynsijärvi et al. 2024), the free registration process for EU root certificate service provider maintained by the European Commission was based on exchange of Excel spreadsheets between the applicant and the service provider and proceeded as described below:

(1) sending a request to register a C-ITS station to Atos

(2) obtaining confirmation of the registration request and receiving EU Root CA & Sub-CA SaaS agreement from the certificate service provider

(3) sending the completed and signed agreement and the official registration certificate of the applicant organisation to the CA

(4) receiving confirmation of the approval of the use of the certificate service

(5) finally, the operator creates a key pair and forwards its public part to the certificate service provider, defines service-specific permits, the stations are registered in the PKI system and the necessary data is configured in the C-ITS station (key and service-specific authorisations that must match the C-ITS messages sent by the registered station).

In the same project, the process was also implemented with the help of a private root certificate service provider. The final report of the project highlighted that the web-based portal offered by the private sector provider for the registration and certificate management of C-ITS stations facilitated and accelerated the registration process of C-ITS stations. The registration process was further accelerated by the automated registration components implemented by the C-ITS station manufacturer (scripts embedded in the station), which enabled the C-ITS station to automatically exchange data with the API of the certification service provider (Microsec).

In both cases, i.e. the EU root certificate service and private provider’s service, the registration authority also had to carry out manual work stages related to the configuration of the C-ITS station.

The following factors should be considered when selecting a root certificate service.

- There is no certainty of whether the EU root certificate service will continue. However, it is generally not intended for large-scale production environments, and the current method of using the service based on Excel file transmission is somewhat slow and cumbersome compared to the services offered by commercial providers. The service is free of charge.
- Private certificate operators offer simpler web-based service portals for registering C-ITS stations and managing certificate services (also Atos, which provides the free EU root certificate service). While the certificate services of private operators are subject to a fee, they may also offer free or very affordable services for small-scale and individual L0 level pilots.

- For small-scale or one-off environments, it is easiest to use the shared service environment offered by root certificate service providers. Based on discussions with service providers, this model works quite well even in larger environments.
- If the intention is to access solely to dedicated certificate environment, a SaaS-based service model can still be used, in which the service provider establishes a separate service environment for the customer. For example, this model has been used to implement national (e.g. Czech Republic), city-specific (Hamburg) or organisation-specific (e.g. Autobahn or ASFINAG) certificate services.
- If the implementation of the certificate service using SaaS model is perceived to pose risks to national or organisational security, establishing a root certificate service within a country's or organisation's internal data centre can be considered (on-premises model). However, the establishment of such as service requires preparation for higher costs, the establishment (or procurement) of a high-security data centre environment, assuming a larger role in the management of the environment and adopting continuous approval procedures in accordance with the EU CCMS.

5.7 Cost analysis

This section discusses the costs of deploying the EU CCMS at the national level. In practice, the costs of implementing the EU CCMS can be divided into the following areas.

(1) The deployment and operational management of the national central C-ITS station and interchange server.

(2) Possible establishment of a centralised national root certificate service and use of certificate services.

(3) Costs incurred by C-ITS station operators in connection with security and certificate policy requirements.

The cost element in item 1 is based on a research line related to a long-range communication solution that strongly guides the present study. The cost elements in items 2 and 3 are not dependent on the technical implementation of the C-ITS architecture (long-range or short-range communication option).

Cost generation and allocation are also associated with a significant number of national choices, which affect the generation and distribution of costs between the different members of the C-ITS ecosystem. These choices are partly highlighted in this cost analysis, but they have also been mentioned in the previous chapters of this report.

It should also be noted that these cost components do not yet mean that any C-ITS services have been deployed and produced. These costs are incurred from the basic infrastructure services necessary for the implementation of the C-ITS system in accordance with the EU CCMS and the C-ITS Security and Certification Policies, as well as requirements set for operators to develop their actual C-ITS services.

5.7.1 Central C-ITS stations and interchange servers

Three different methods can be roughly identified for the deployment of Central C-ITS stations and interchange servers: (1) in-house development, (2) purchasing a product or service from the market, (3) community-driven open-source development.

The implementation of the national central C-ITS station may also be closely associated with the implementation of the national interchange server. More detailed requirements for an interchange server are discussed in Chapter 7 of this report.

Table 6. Estimated costs based on an expert interview with Fintraffic Road Oy for the development and deployment of the central C-ITS station and interchange server based on own development work (Fintraffic interview 2024)

Cost type	Explanation	Cost estimate
Development of a central C-ITS station and interchange server	The development of the central station is based on an estimate of a development project lasting approximately two years with the minimum resourcing of 7 full-time equivalents (FTE). Example of a potential development team: 1 chief technical architect, 2 back-end developers, 1 data warehouse expert, 1 UI developer and other tasks and roles amounting to 2 FTEs (project management, quality, UX design, cloud or server architecture, interface development). The work also includes the definition and approval of the protection profile in accordance with ISO 15408 (Common Criteria), the assessment of the information security level and interoperability testing enabled by ETSI (participation in an ETSI Plugtest event).	approx. EUR 2,000,000–2,500,000
Continuous costs	24/7 operation of the ICT infrastructure, ITIL-compliant (IT Infrastructure Library) management services (disruption management, problem management, etc.), 15 min response time (NIS2 critical system). Estimate EUR 300,000/year. Platform security management service, version management, planning, testing and implementation of new security updates on a monthly basis. Estimate approx. EUR 200,000/year. Capacity services (cloud or server platforms, physical duplication, load balancing, database capacity, security modules, communications). Estimate EUR 150,000/year.	approx. EUR 900,000/year

<table>
<tr><td></td><td>Continuous software lifecycle management (software bug fixes and software security updates), new features and necessary development needs (e.g. EU and national integrations), continuous development input of approximately two people. Estimate EUR 250,000/year</td><td></td></tr>
<tr><td colspan="3">Notes:
The two-year period proposed for the development of the central C-ITS station and the interchange server reflects an active and efficient specification and development period. The project is very likely to involve several delays, including those related to decision-making and the Common Criteria assessments, as well as ETSI interoperability tests, which prolong the actual implementation time of the project.
Own development work can be accelerated by making use of possible open-source platforms, which can be used as a basis for the development project and the efforts to develop the operator’s own code implementation. To counterbalance the faster progress of development work, the operator will have to take responsibility for software implementation, which is often highly extensive and may include software errors and information security problems. The open source community (or other entity) that developed the original code often does not provide support to developers regarding the original code, and the developer must start developing its own implementation on the basis of the open code (although this process may not involve anything negative, as it is a very common course of action in the open source world).
Another alternative involving open source code is to establish or join a community activity, which is described below as a distinct option in a bit more detail, and especially in Chapter 7 of this report.</td></tr>
</table>

Table 7. Below is an estimate of the cost structure of the procurement of a central C-ITS station and interchange server purchased as a ready-made product. These estimates are based on the working group's own assessment.

Cost type	Explanation	Cost estimate
Deployment of a central C-ITS station and interchange server	The service provider establishes a customer-specific domain in its service environment (a shared service in which customers are itemised by means of access management) or a customer-specific local operating environment (also in terms of the hardware platform).	approx. EUR 500,000–1,000,000
Continuous costs	User license for the environment delivered as a service.	approx. EUR 250,000–500,000/year
Notes: The pricing principles of the environment delivered as a service may vary significantly from one service provider to another. Costs may be bound based on the number of C-ITS stations connected to the system or the capacity used. Cost models may also be significantly influenced by the specifications attached to the tendering process by the customer. For example, the service provider may be requested to indicate prices using a specific structure, such as a fixed annual cost with an annual price adjustment allowance or a price breakdown according to the number of devices joined to the environment. The number of products emerging in the sector (competition) also affects pricing and price development in the private sector. The benefits related to procuring the product include the clearly less demanding launch of the service, the automatic development of the product and its compliance with new requirements and standards without separate costs. These benefits are counterbalanced by having less control over product development and prioritisation.		

Table 8. Below is an estimate of the implementation of a central C-ITS station and interchange server based on community-driven open-source development.

<table>
<tr><th>Cost type</th><th>Explanation</th><th>Cost estimate</th></tr>
<tr><td>Development of a central C-ITS station/interchange server</td><td>In practice, the requirements for the development of the actual product or solution are at least the same as those for a product based on own development presented in Table 6. The product is implemented based on a different model, which makes it very difficult to estimate costs. In practice, the work is carried out as part of a community, and all community members contribute to the development work. As a rule, it can thus be assumed that the cost of own contribution is lower compared to development carried out alone. On the other hand, the actual cost depends on issues such as the community's size, objectives, consistent vision of the product, desire to invest in co-creation, the success of co-creation management, etc.</td><td>-</td></tr>
<tr><td>Continuous costs</td><td>Estimating the costs of further development and maintenance involves many similar difficulties as in the previous development phase.</td><td>-</td></tr>
<tr><td colspan="3">Notes:
The community-like activities could be based on the desire of several countries (e.g. the Nordic countries) to develop a central C-ITS station and interchange server in cooperation. This would involve establishing a common open source community, which would also involve a commonly agreed governance model.
To manage the administration of such an open community, it is common to procure the services of a provider specialising in the management of open source communities, including software repositories, version control platforms, collaboration and the central coordination of development efforts.
Community-like activities have significant benefits compared to the use of open source platform codes as a part of in-house development. Each participant within the community is responsible for their own contribution and provides support to other members of the community in potential problems related to their contribution. The community is responsible for ensuring the interoperability of all parts of the project and testing the solution that it builds together. In other words, working within the community will provide better support for the source code of the final product and if the members of the community have a clear and consistent view of the direction of the solution they are developing, everyone will benefit fully from the work done by the community members.
One of the drawbacks of community-based work is the slow initiation of development activities. It may take time to establish the community and agree on its joint management and development principles.
These features of development carried out in an open-source community are discussed in more detail in Chapter 7.</td></tr>
</table>

5.7.2 Root certificate service

The costs produced by a root certificate service vary considerably based on which implementation model will be selected nationally. This particularly affects the distribution of costs between different operators on the one hand and the ability to manage the use, registration and management of service-specific authorisations of C-ITS stations on the other.

It is possible to select a model that does not involve setting up a national root certificate service but rather allows each party to manage their certificate activities with the root certification authority of their choice. The operating principle of the EU CCMS enables this model, and it is also feasible from the perspective of the management of service-specific authorisations. The authorisations must be applied for from one (agreed) central government body, and proof of obtaining the authorisations must be handed over to the applicant to enable the selected root certificate service provider to issue authorisations for approved C-ITS services to the registered C-ITS stations in connection with registration.

Another option is to establish a national root certificate service in Finland, which is used by all Finnish road operators. A decision may also be made to offer this to other members of the C-ITS ecosystem. Such a centralised model improves the management of the distribution of service-specific authorisations and root certificates, as it enables planning the management process smoothly at the national level. Meanwhile, it prevents a situation in which every Finnish operator registering C-ITS stations (C-ITS station operator) needs to initiate its operations by searching for a root certificate service, launching a competitive tendering process and concluding a contract with the service. This model also leaves room for making decisions on whether the use of the national root certificate service would be subject to a fee.

This assessment does not take the free EU root certificate service into consideration, as based on the report working group and expert interviews, it is understood that this service is not intended for certificate services for large-scale and long-term C-ITS systems.

Table 9. Various cost estimates for the implementation of a national root certificate service. The assessments are partly based on expert interviews with root certificate service providers (Teskalabs interview 2024, Microsec and Commsignia interview 2024.

Cost type	Explanation	Cost estimate
The establishment of a **shared SaaS PKI** root certificate service	The root certificate service is purchased as a cloud-based service from a service provider that establishes a new customer relationship in the certificate service and establishes administrators and users according to the customer’s needs. The operating environment is shared with other customers of the service provider.	approx. EUR 10,000
Operating costs of the **shared SaaS PKI** root certificate service	The SaaS solution is provided entirely as a service and the customer does not have to worry about related infrastructure costs, system development, changes in EU CCMS requirements or annual audits. The customer also has the opportunity to influence these costs through the requirements of the competitive tendering process (e.g. a fixed monthly price valid throughout the contracting period or the number of C-ITS stations registered as the basis for the price as a requirement, etc.). According to the expert interviews, pricing is commonly based on the number of registered C-ITS stations. At the same time, service providers have also come across other types of models, such as annual fixed costs based on the number of devices estimated in advance. In this case, costs have been estimated based on the assumption that the national C-ITS ecosystem has launched its operations and passed the initial development phase, where the number of registered devices may be still very low.	approx. EUR 25,000–100,000
The establishment of a **customer-specific SaaS PKI** root certificate service	The root certificate service is purchased as a cloud-based service from a service provider that establishes a new customer-specific (dedicated) certificate service environment. The service provider obtains approval for the new root certificate service under the EU CCMS and establishes the software and user IDs and structures required for the customer relationship. The model provides better opportunities, e.g., in terms of the versatility of user group management. The management environment also lends itself to the establishment of several system administrators who only have access to the device view of the group specified for them (e.g. a city).	approx. EUR 25,000–100,000

Cost type	Explanation	Cost estimate
Operating costs of the **customer-specific SaaS PKI** root certificate service	The service provider operates and offers the certificate service from its own server or cloud service platform, and provides the customer with tools for the management of certificates and users as well as support services for using the system. The service provider is also responsible for the annual audit requirements related to the EU CCMS and for any change needs related to the new requirements.	approx. EUR 50,000–200,000
Establishment of a **local PKI** root certificate service (on-premises)	The local implementation option for root certificate services is based on the establishment of a complete root-service infrastructure based on the location chosen by the customer, including server infrastructure and software installation (on-premises). This model provides complete control of the root certificate service but requires significant expertise, major investments in hardware such as HSM modules where keys are stored as well as a redundant and geographically distributed architecture. Sub-certificate services must also be kept physically separate from each other. All levels of the root certificate service environment must be approved in accordance with the EU CCMS requirements (including data centre, server and software infrastructure).	approx. EUR 500,000–1,000,000
Operating costs of the **local PKI** root certificate service (on-premises)	The operating costs of a locally implemented root certificate service are determined in a very different way compared to those of a SaaS solution. In this model, the continuous costs consist of the operating costs of capacity services (servers, databases, firewalls, telecommunications and continuous 24/7 system monitoring and management services, critical response time response services, ITIL process management service) and continuous auditing requirements for the environment and the expert work required to perform all these functions. This means that the customer will be responsible for a significant part of all responsibilities related to operational management of the solution, even though support services are available through an external partner for the operational management of the service, the fulfilment of the requirements under the EU CCMS and annual audits. The cost estimate is based on an estimate of the price of the continuous services for the central C-ITS station and the interchange server, as well as an estimate of the impact of annual audits and other EU CCMS requirements.	approx. EUR 250,000–500,000

5.7.3 Operational management of C-ITS stations

The costs incurred by C-ITS station operators mainly consist of the acquisition or development costs of the actual C-ITS stations, the development and deployment costs of C-ITS services and the costs related to the operational management of C-ITS stations.

This section does not comment on the deployment costs of C-ITS services (procurement and deployment of stations), but only on the costs incurred by the C-ITS station operator due to the requirements of the C-ITS Security Policy. In practice, this refers to the certification requirement for information security management systems (ISMS), which is described in Section .4.2.2 of this report.

Below is a brief summary of the ISMS requirements for C-ITS station operators set by the C-ITS Security Policy:

- A general requirement is a certified information security management system according to ISO-27001.
- For parties operating vehicle C-ITS stations, this requirement may be replaced by a cybersecurity management system certified in accordance with UN Regulation R155 (UN Regulation No. 155 2021).
- C-ITS station operators operating an essential road transport service may apply the requirements of the NIS1 and NIS2 Cybersecurity Directives to information security management.

This cost estimate does not distinguish between the costs of obtaining a certificate and certificate maintenance for these different systems. The cost estimates are based on information generally available in the sector, the cost estimates used and the expertise of the working group.

Table 10. Costs incurred by C-ITS station operators for the development and certification of information security management systems (ISMS) and the maintenance of the system and certificates.

Cost type	Explanation	Cost estimate
Development and certification of the ISMS	Development of the ISMS, including the development of the organisation’s information security management and leadership models, the development of operating methods, any new IT equipment and system investments, any necessary consulting services and the time spent on the project in the organisation. The duration of the project is generally estimated to be approximately 1–2 years, depending on the size of the organisation and its initial level of information security management.	approx. EUR 50,000–100,000
Maintenance costs of the ISMS	This section mainly includes the working hours spent on annual system audits and auditing fees related to the ISMS.	approx. EUR 10,000–30,000

Notes:

The above share of maintenance costs does not comment on the cost structure of companies' continuous operative activities, which the ISMS typically affects by increasing the internal costs of the company (depending on the initial level of information security management at the company before certification). Potential effects include higher administrative workload related to information security reflected in the company's operations (e.g. information security, teams for leading risk management work, new practices related to information security management visible in planning work as well as personnel training and instructions related to information security management), operating costs of new IT systems, and higher information security management requirements related to project and service operations set by the ISMS. The costs of new tasks related to information security management are strongly linked to the size of the organisation. The costs resulting from these new tasks, action groups and new practices taken into account in work typically far outweigh the costs of system auditing and system maintenance presented in the above table. For example, in an organisation with 50 employees, if the new practices require four extra hours of each employee's time each month, this would result in an additional annual cost of almost EUR 150,000 related to information security management (4 x 50 x 12 x EUR 60 per hour).

Chapter 5.3 described the indirect impacts of certification requirements on the entire intelligent transport sector. These requirements also apply to companies whose work revolves around C-ITS services, as it is highly likely that the certification requirements for C-ITS station operators will also apply to private sector operators providing solutions or services to C-ITS station operators in relation to the development, operation, maintenance and upkeep of C-ITS systems.

It is possible to aim to minimise the costs to C-ITS station operators described in this section through the means of technical architecture design. In the long-range communication option, solutions can be developed in a way that ensures that the responsibility for the operational management of C-ITS stations is focused solely on the party responsible for the operational management of the central C-ITS station. This means that only the central C-ITS station generates C-ITS messages, in which case the initial data for generating the messages is delivered in other ways. Examples include the utilisation of a National Access Point (NAP) to share up-to-date traffic data and minimum traffic safety information and the transmission of traffic light data to the national central C-ITS station through a secure communication method specified at the national level (not through a roadside C-ITS station).

An example of the use of the National Access Point (NAP) is the requirement under the ITS Directive to transmit SRTI and RTTI data to the NCP. Roadworks warnings (RWW) services can be implemented so that road contractors are required to transmit (only) SRTI data to a NAP as part of the competitive tendering process. From the NAP, the data can be transferred to the national central C-ITS station and to other C-ITS service provider interfaces maintained by private operators that use the data to generate RWWs and distribute them via mobile networks to vehicles approaching roadworks. This allows for avoiding any requirements or costs to the maintenance contractor related to C-ITS station operation (e.g. procurement of roadside C-ITS stations and requirements related to their operation). This topic is discussed in more detail in Chapter 11 of this study.

6 Central C-ITS stations and signing messages

6.1 Introduction

The central C-ITS station is one of the four types of C-ITS stations included in the reference architecture of ETSI EN 302 665. It is software-based solutions that operates in cloud environment or data centres and serves as an important back-end system for C-ITS service deployments. These stations also play a key role in enabling the operation of C-ITS services. They collect data on the status of the transport network and vehicles and generate C-ITS messages by using various data sources and transmit messages between regional C-ITS systems. They also provide C-ITS services to road users and offer a real-time situational overview of the state and operation of the transport network to external systems, such as traffic control and situational awareness platforms. In IP network-based long-range communication solutions, the role of central C-ITS stations will increase significantly compared to short-range communication solutions. They generate and transmit C-ITS messages over an IP network as central communication nodes between infrastructure and vehicles. In generating C-ITS messages, the central stations use input data from vehicle or roadside ITS stations or from outside the C-ITS system.

In IP network-based C-ITS systems, central C-ITS stations may process significant amounts of input data, using them to generate C-ITS messages and transmit large amounts of messages between regional central C-ITS stations and interchange servers. When a central C-ITS station complies with the EU C-ITS Security Credential Management System (EU CCMS) regulations, it signs C-ITS messages as they are generated and transmitted and verifies their integrity and confidentiality upon reception by checking their digital signatures. The operation may require signing or verification of signatures for a large volume of messages. These cryptographic tasks require substantial computing power on central stations. In the worst-case scenario, this computationally intensive workload of C-ITS stations may reduce the performance of the system providing C-ITS services.

Requirements related to the operation and manufacture of central C-ITS stations are specified earlier in this document in Chapter 4. Chapter 3 presented the EU-wide EU CCMS system, based on PKI certificates, to be implemented in European C-ITS systems. EU CCMS will define how certificates intended to secure C-ITS communications are managed, distributed and used.

This chapter focuses in more detail on the role of the central C-ITS stations as a part of the C-ITS system, communication between the central stations and signature measures related to communication to ensure the confidentiality and integrity of data. This chapter presents an overview of C-ITS communication based on the C-ITS architecture defined by the C-Roads Platform. It describes communication options, outlines security implementation principles, and assesses how message signing affects the performance of C-ITS services and central C-ITS stations. The chapter also includes an imaginary example of the national architecture of C-ITS service implementations based on long-range communication.

6.2 Overview of C-ITS communication

6.2.1 C-ITS communication solutions

The objective of the C-Roads Platform is to create a harmonised technical architecture for C-ITS service to ensure their seamless operation across Europe. This objective is supported by the specifications related to IP-based network implementations set out in the C-ITS IP Based Interface Profile (2024). The specification presents the different options related to C-ITS communication and the use of C-ITS security credentials defined in the EU CCMS. In addition to a general description of communication, the specifications include the definition of the key components of the C-ITS service implementation architecture based on IP networks, the connections between central C-ITS stations and interchange servers, cooperation and the technical operation of the interfaces used, which are discussed extensively here and in the following Chapter 7 of this study.

Figure 2 below shows an overview of C-ITS communication as defined by C-Roads Platform. The figure shows the different elements of the C-ITS service implementation architecture and the requirements for the use of a certificate for signing C-ITS messages defined in the EU CCMS.

As shown in Figure 2, C-ITS messages are signed in the communication between the roadside station and the vehicle station that uses the ITS-G5 communication method (lower right corner) and for communication between central C-ITS stations that use IP-based communication (upper left corner). As shown in the figure, road operators can freely choose the communication method between the roadside C-ITS stations and the central station (upper right corner), and signing messages according to the EU CCMS is not required. Similarly, service providers are free to choose how central C-ITS stations (central C-ITS station A in the figure) communicate with end-user terminals such as mobile device or vehicle C-ITS station.

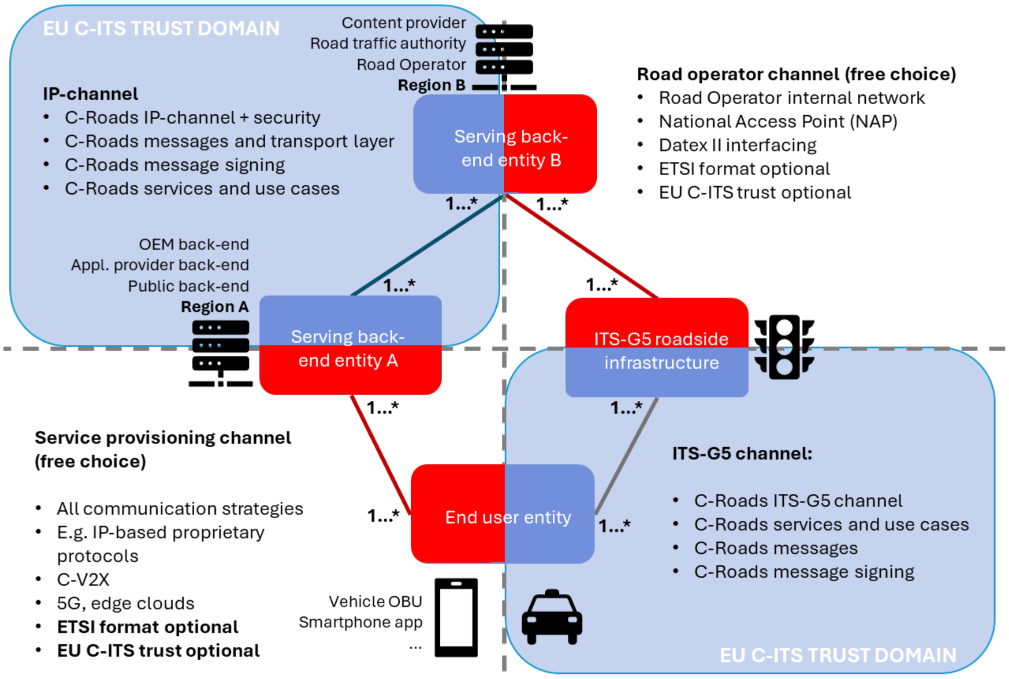

EU C-ITS TRUST DOMAIN
Content provider
Road traffic authority
Road Operator
Region B
IP-channel
• C-Roads IP-channel + security
• C-Roads messages and transport layer
• C-Roads message signing
• C-Roads services and use cases
Serving back-end entity B
1...*
1...*
Road operator channel (free choice)
• Road Operator internal network
• National Access Point (NAP)
• Datex II interfacing
• ETSI format optional
• EU C-ITS trust optional
OEM back-end
Appl. provider back-end
Public back-end
Region A
1...*
1...*
Serving back-end entity A
ITS-G5 roadside infrastructure
1...*
1...*
Service provisioning channel (free choice)
• All communication strategies
• E.g. IP-based proprietary protocols
• C-V2X
• 5G, edge clouds
• ETSI format optional
• EU C-ITS trust optional
1...*
End user entity
1...*
ITS-G5 channel:
• C-Roads ITS-G5 channel
• C-Roads services and use cases
• C-Roads messages
• C-Roads message signing
Vehicle OBU
Smartphone app
...
EU C-ITS TRUST DOMAIN

Figure 2. Overview of C-ITS communication according to the C-Roads Platform specification (adapted from C-ITS IP Based Interface Profile, 14).

The requirements for using C-ITS security credentials defined by the EU CCMS and the C-Roads Platform play a key role in message signing, C-ITS stations, and network resource management. This topic is discussed in more detail in section 6.4 of this report. The following sections provide a more detailed description of the various communication solutions used in C-ITS implementations.

6.2.2 Short-range communication

The short-range communication solution is based on the use of ITS-G5 technology, which is the European standard for short-range communication between vehicles and between vehicles and roadside stations (Figure 2, lower right-hand corner).

The ITS-G5 standard is based on 802.11p technology, which is one version of the IEEE[1] 802.11 Wi-Fi standard series developed for use in a cooperative transport system. In the United States, the term Dedicated Short-Range Communications (DSRC) began to be used for 802.11p technology. In Europe, the same DSRC term was initially used as a part of the ETSI/CEN standardisation (2010), but later in the 2010s, the term ITS-G5 was adopted to refer to the technology. The communication mode (physical and communication layers) of the ITS-G5 technology is defined in ETSI EN 302 663, whose latest version was published on 1 July 2020 (version 1.3.1).

The technical reference architecture for short-range communication of C-ITS stations - including communication layers, interfaces and interoperability requirements based on OSI model[2] - is defined in detail in the ETSI EN 302 665 and ISO 21217 standards.

The development of a short-range communication solution based on radio technology has especially focused on vehicle-to-vehicle communication. It is optimized for high-speed communication between stations and for low communication delay requirements. ETSI ITS-G5 C-ITS stations use the 5.85-5.925 GHz frequency band that enables them to communicate omnidirectionally within a radius of 300–1000 m from the transmitting station. The frequency of C-ITS messages vary depending on the message type, typically between 0.1 and 10 Hz. (C-Roads WG2 Deployment Documentation 2024)

When using the ITS-G5 communication mode, the EU CCMS is an essential element to ensure the authenticity of messages, as messages are transmitted over the radio similarly to a ‘broadcast’, which means that they can be received and transmitted by anyone operating in this frequency band.

[1] IEEE (Institute of Electrical and Electronics Engineers) is the world’s largest professional organisation that developed and published the first standard for wireless Ethernet in 1997. Version 802.11p for ITS (Wireless Access in Vehicular Environments (WAVE)) was released in 2010.

[2] The Open Systems Interconnection (OSI) model is a common reference model used in telecommunications technology that describes the operation of the seven layers used to communicate over a network. Each layer plays a specific role in the implementation of communications. The OSI model was defined by the International Telecommunication Union (ITU-T) in 1984. The layers of the OSI model will be hereinafter referred to as OSI-x, where x refers to the layer number of the OSI model.

In ITS-G5 communication, C-ITS messages are generated and digitally signed according to the EU CCMS, either by an in-vehicle ITS station or a roadside ITS station. For short-range C-ITS communication, the signing process workload is spread across many C-ITS stations. In this setup, all available communication bandwidth and computing power of C-ITS stations are dedicated to C-ITS services, with no competing applications sharing these resources. However, the operating range of radio technology used for short-range communication is limited, which means that an extensive network of roadside stations is needed to cover the entire road network. In countries using ITS-G5, roadside ITS stations are typically located within one or a few kilometres of each other on the road network. Achieving uninterrupted coverage would require an even denser network of roadside ITS stations. In urban environments, the distance between stations may need to be significantly shorter due to the high frequency of short-range communication, which makes it sensitive to interference caused by obstacles between the sender and recipient. The “line-of-sight" principle, referring to an unobstructed connection between communication parties, is considered a general requirement.

The short-range communication solution also includes a section implemented with the IP network between the roadside C-ITS stations and the central C-ITS station. This is shown in the upper right corner of Figure 2. The purpose of this section is to produce data on the status of vehicles and the transport system (e.g. vehicle location, speed and direction, behaviour, traffic network disruptions) to central C-ITS stations in the C-ITS based on short-range communication. Meanwhile, the central C-ITS stations produce data to be used in traffic situational awareness, analysis and control systems outside the C-ITS system.

In this solution, vehicle stations communicate information to roadside C-ITS stations using ITS-G5 technology. Roadside C-ITS stations typically transmit data to the central C-ITS station via a closed and fixed IP network (e.g. a road operator network).

6.2.3 Long-range communication

In C-ITS, long-range communication refers to the transmission of messages between vehicles and infrastructure via fixed IP networks and mobile networks. The solution aims to use mobile networks to provide C-ITS services to road users to avoid the need to equip roadsides and streets with a large number of roadside C-ITS stations.

The long-range communication solution is based on the evolution of commercial mobile phone networks utilising 3G technology to 4G technology, which became the standard in the 2010s (also known as 4G LTE, Long-Term Evolution) and the 5th generation of mobile network technology utilising 5G technology, which is currently widely used (also known as 5G NR, New Radio). The marked improvement in the performance of the new mobile networks and the reduction in delays thanks to increased capacity have created an opportunity to make effective use of these technologies in communications between infrastructure and vehicles.

In accordance with the C-Roads Platform specifications, the long-range communication system consists of central C-ITS stations, typically interconnected by wired IP networks (e.g. the Internet or other closed IP-based network implementation), as shown in the upper-left corner of Figure 2. C-Roads Platform defines the Basic Interface (BI) used for communication between central C-ITS stations, the Advanced Message Queuing Protocol (AMQP) used for communication, the structure of C-ITS messages and the requirements for signing them (in accordance with the EU CCMS). (C-ITS IP Based Interface Profile 2023)

In C-ITS solutions, the Basic Interface is intended for the real-time data exchange between back-end systems. Together with the AMQP protocol, it provides a harmonised, open and jointly specified method of communication between central C-ITS stations. AMQP is an open application-layer protocol (Layer 7 of the OSI model), standardised by OASIS[1] in 2012, and is designed to enable efficient, reliable messaging and queuing in distributed systems.

Signing messages under the EU CCMS ensures the integrity of messages transmitted by the central stations and the reliability of the sender. In large-scale C-ITS architectures, central stations may need to process a high volume of messages. Consequently, signing and verifying messages can place significant demand on their computing resources. This topic is discussed further in Section 6.4.

In solutions based on long-range communication, central C-ITS stations play three key roles: (1) central C-ITS stations use a variety of data sources to generate C-ITS messages, (2) central C-ITS stations communicate messages between different C-ITS stations (communication between central stations) and (3) central C-ITS stations provide actual C-ITS services to end-users.

National Access Points (NAPs), which provide extensive data on the transport network’s status, are identified as key sources of information for generating C-ITS messages in the future. A wide range of SRTI and RTTI[2] data on the state of the transport network is submitted to NAPs by road operators, municipalities and other private entities that hold significant amounts of traffic data. C-ITS messages can also be generated extensively based on a wide range of other data sources (e.g. existing traffic control systems, real-time traffic measurement and identification systems, data collected through crowdsourcing or data transmitted by integrated vehicle C-ITS stations supporting mobile network communication). National Access Points (NAPs) are further discussed in Section 6.2.5.

[1] OASIS (Organisation for the Advancement of Structured Information Sharing) is a non-profit organisation consisting of industrial operators, public sector actors and research organisations. The AMQP protocol developed by the organisation has also been published as an ISO standard in 2014 (ISO/IEC 19464 2014) and as an open specification published by the OASIS organisation (OASIS AMQP Protocol Specification 2012).

[2] The requirements related to the EU-wide provision of SRTI and RTTI (Safety Related Traffic Information and Real-Time Traffic Information) are defined in the original ITS Directive (2010/40/EU) and the supplementary delegated regulations (RTTI: EU/2015/962 and EU/2022/670, SRTI: EU/886/2013). The gradual deployment of the transmission of SRTI and RTTI and the NAPs is regulated by the revised ITS Directive (EU 2023/2661 2023).

As shown in the lower-left corner of Figure 2, in long-range communication solutions, commercial mobile networks such as 4G or 5G are typically used for communication between vehicles and central C-ITS stations. However, technologies or network protocols used are not specified in more detail. In this model, C-ITS services can be provided to vehicles either through mobile applications or through in-vehicle C-ITS stations that support mobile connectivity.

C-Roads Platform specifications do not define the technical implementation architecture of actual data networks in long-range communication solutions. In practise, the back-end services of C-ITS system using long-range communication – such as national and regional central C-ITS stations and interchange services - can be placed in a public open IP network. However, using the public Internet may limit the service level of communication between C-ITS stations, as it does not guarantee performance in terms of latency or connection availability. Moreover, services deployed in the public networks are exposed to disruption attempts, such as distributed denial-of-service (DDoS) attacks, which have become a common cause of service disturbances. In long-range communication solutions, delivering C-ITS services over mobile networks may also face quality issues. While mobile networks generally provide sufficient performance for most C-ITS services under normal conditions, they do not guarantee a specific service level of service, similar to the public Internet. Another problem identified in relation to mobile networks is potential blind spots in the network. (Kilpiö et al. 2024)

A later section of the study (Chapter 0) provides a more detailed examination of communications network solutions.

6.2.4 Hybrid communication

Hybrid communication refers to the implementation of C-ITS systems that combine both short- and long-range communication solutions. This approach enables C-ITS services to operate simultaneously via IP networks, central C-ITS stations and mobile networks (long-range communication solution), as well as via roadside C-ITS stations and vehicle C-ITS stations using radio technology (short-range communication solution).

The special benefits of hybrid communication include the possibility to use various communication methods in different C-ITS services. Services requiring particularly high real-time operation and network operations subject to strict service level requirements could be implemented by means of locally installed roadside stations, which would only need to be installed in certain areas that are essential for these services. At the same time, less time-critical C-ITS services requiring extensive geographical coverage could be implemented using IP and mobile networks. Hybrid technology enables vehicles to communicate with each other and roadside equipment using a short-range communication solution as well as with central C-ITS stations using the mobile network.

The C-Roads Platform also recognises hybrid solutions that transmit C-ITS messages to end users via multiple communication channels, using a short-range communication solution based on ITS-G5 technology and a long-range communication solution based on IP and mobile technologies (Figure 2, p. 59).

The hybrid technology-based communication solution has been particularly promoted by the 3GPP1 (Third Generation Partnership Project) developing mobile network technologies. The results of these development efforts are called C-V2X (Cellular Vehicle-to-Anything) technologies. The name refers specifically to the extensive utilisation of mobile network technologies in all communication situations in cooperative transport systems.

C-V2X technologies are based on mobile network technology, which provides direct communication between vehicles as well as between vehicles and roadside stations using a short-range communication solution in the 5.9 GHz frequency band. At the same time, it utilises a commercial mobile network solution for long-range communication.

To date, the 3GPP project has already defined a C-V2X technical specification LTE-V2X based on 4G networks, which has also been integrated into ETSI standards ETSI TS 136 331 and ETSI TS 136 414. In this context, the short-range communication interface is called the PC5 interface (or LTE-V2X Direct), while long-range communication utilising the mobile network uses the Uu interface. The short-range communication version of this technology has also been piloted in Finland (Kynsijärvi et al. 2024).

The specification work on NR-V2X technology based on 5G networks (New Radio V2X) is also well underway. In this technology, the short-range communication interface is called the NR sidelink interface, and long-range communication is implemented using the NR Uu interface. NR-V2X is part of the broader 3GPP NR-5G specification work ("38 series", Radio technology beyond LTE). Their definition and standardisation as a part of the ETSI standards is still ongoing.

The lack of interoperability between traditional ITS-G5 technology and C-V2X technologies defined by 3GPP is currently seen as a key problem in the spread of hybrid solutions, which means that vehicles equipped with different technologies cannot communicate directly with each other. The same applies to communication between roadside C-ITS stations and vehicles.

The 2019 Delegated Regulation proposal already identified the inclusion of 3G and 4G networks as likely additions to provide Day 1 C-ITS services. The C-V2X solutions defined by 3GPP were identified as possible technology additions to Commission Regulations, although the interoperability requirement with existing technologies (i.e. ITS-G5) was also mentioned (EU C/2019/1789 2019, paragraph 30). The C-Roads Platform has continued to advance these concepts through its specification work.

[1] 3GPP is an extensive cooperation project established in 1998, focusing especially on developing technologies based on mobile network technologies for the needs of IoT applications. 7 standardisation organisations (including ETSI) and market partners such as 5GAA (5G Automotive Association), which brings together automotive, technology and telecommunications operators, are involved in the work.

Following the proposed Delegated Regulation, C-V2X technologies have evolved significantly, with 4G-based version now integrated into ETSI standards. At the same time, clear policies for adopting C-V2X have been established in both Asia and America. For example, in November 2024, the U.S. Federal Communications Commission (FCC) approved the use of C-V2X technology in the 5.9 GHz frequency band (FCC C-V2X Auto Safety Spectrum Rules 2024). Car manufacturers have also expressed a clear interest, particularly in NR-V2X technology, which is based on 5G technologies and is still under development.

At the same time, some European countries – particularly in Central Europe - have already made significant investments in ITS-G5 technology, leading to the emergence of related ecosystems. For example, major road operators Autobahn (Germany) and Asfinag (Austria) have equipped motorways with significant numbers of ITS-G5 roadside stations (TEN-TEC EU central C-ITS stations 2025). For example, more than 500 ITS-G5 roadside stations have been installed on Austrian motorways by the end of 2024 (on average one for every four kilometres). At the same time, in addition to making investments in roadside stations, Autobahn has invested in the development and deployment of intelligent roadworks trailers. The aim has been to equip approximately 1,200 intelligent roadworks trailers with ITS-G5 technology by the end of 2024 to produce roadworks warning services for approaching vehicles as C-ITS messages. In the period 2019–2024, the German car manufacturer Volkswagen has already equipped more than 1.3 million cars with ITS-G5 support. (C-Roads Platform webinar 2024)

Although Europe has been developing a common European C-ITS system for over a decade, the incompatibility of two key technologies can cause major problems in the deployment of C-ITS services - especially if different countries and car manufacturers commit to different technologies. At the same time, there have been expectations for the Commission to take a clear stance on the matter, ideally by issuing a new delegated regulation outlining the requirements for the European C-ITS system.

6.2.5 Utilisation of the National Access Point (NAP)

Section 6.2.3 on long-range communication already highlighted the role of the National Access Point (NAP) as a part of the architecture of C-ITS service implementations. As this solution plays such a key role in the implementation of C-ITS services, it is discussed separately in this dedicated section.

The National Access Point (NAP) is an entity separate from the C-ITS ecosystem that plays a broader role in the open distribution of road transport-related data while developing the ITS sector and related systems. As an independent system, it is therefore not part of the C-ITS system and not subject to the same requirements. However, the types of data to be transmitted to the NAP can be used to generate C-ITS messages, thereby enabling the provision of C-ITS services. On the other hand, the type of data produced by the NAP can also be produced by the C-ITS system, so there is good reason to examine the possible synergies between these entities.

The development requirements of the National Access Point (NAP) are based on the European Commission’s efforts to promote the availability and exchange of road transport data and to support the emergency of safety-enhancing end-user services, including C-ITS services. The regulatory framework for SRTI and RTTI data transmitted to the NAP obliges road managers to provide, in machine-readable format, essential rules and restrictions, information on network status, and safety-related data. These categories include various types of restriction data and information related to hazardous situations, road or traffic lane closures and weather conditions. Therefore, there are clear similarities with the C-ITS service categories defined by the C-Roads Platform. Obligations have also been introduced regarding the planning and implementation of the NAP, with the aim of considering stakeholders as well as new types of data and their specific characteristics. (Laine & Kotilainen 2024)

Traffic data may be provided to the National Access Point (NAP) in different formats, mainly DATEX2, Inspire and TN-ITS formats. The data submitted to the NAP lends itself to generating C-ITS messages in a centralised manner. In C-ITS implementations, central C-ITS stations can access to real-time traffic data via NAP – such as traffic sign information and scope, weather conditions, disruptions, or location of roadworks - and use this data to generate corresponding C-ITS messages.

C-ITS messages generated through the National Access Point (NAP) can be provided to end-users in several ways, depending on how C-ITS system is implemented. C-ITS messages generated by the central C-ITS station can be delivered to end-users via short-range communication by first transmitting them over an IP network to roadside C-ITS stations, which then forward the messages using short-range communication. In other words, end-user accessibility in this solution is entirely dependent on the coverage provided by the roadside station network. In the long-range communication option, messages can be delivered to end-users via mobile networks, by using C-ITS mobile applications developed by service providers or by transmitting the data directly to integrated in-vehicle C-ITS stations. Obviously, this means that the vehicle C-ITS stations must support long-range communication technologies.

When using a National Access Point (NAP) to generate C-ITS messages, the entities responsible for the operational management of central C-ITS stations are responsible for ensuring the reliability of the input data. This responsibility is defined in the C-ITS Security Policy document, discussed earlier in this report in Section 4.2 (operational management of C-ITS stations).

In fact, ensuring the timeliness and quality of the data is a key issue to be resolved to ensure that the data collected to the NAP, and the C-ITS messages generated from it, could be considered a valid implementation model for C-ITS services.

6.3 Implementation of information security

This subsection presents the key elements that ensure message integrity and confidentiality for both short-range and long-range communication, including security aspects of long-range communication. EU CCMS and its principes, based on the C-ITS Certificate Policy for communication security, were described earlier in Chapter 3. This chapter explains information security in more detail by focusing message structures, sessions between the back-end systems used in long-range communication, and message signing.

A separate subsection presents the structure of the C-ITS messages according to the C-ITS Security & Governance specification (2023) from C-Roads' technical working group (Technical aspects). The second subsection presents the principles for signing C-ITS messages, and the third subsection describes the implementation of security for sessions between back-end systems in long-range communication.

6.3.1 Structure of C-ITS messages

A C-ITS message is a real-time message compliant with the EU CCMS, relayed between different C-ITS stations, and containing the data payload of the actual C-ITS service. Figure 3 below illustrates the content of the message in different communication methods.

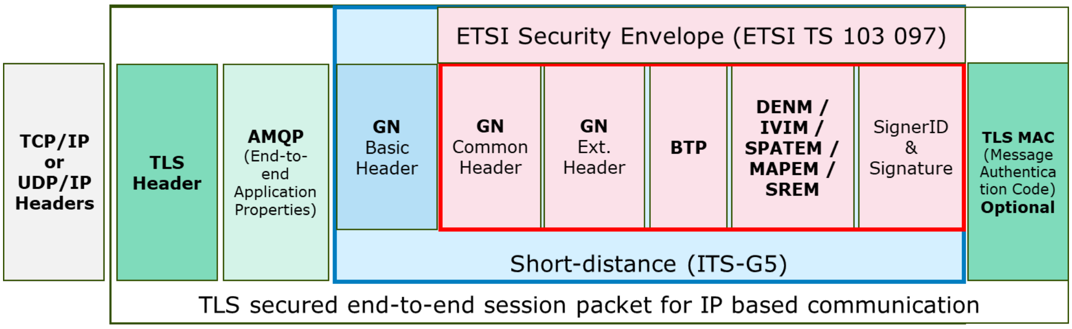

ETSI Security Envelope (ETSI TS 103 097)
TCP/IP or UDP/IP Headers
TLS Header
AMQP (End-to-end Application Properties)
GN Basic Header
GN Common Header
GN Ext. Header
BTP
DENM / IVIM / SPATEM / MAPEM / SREM
SignerID & Signature
TLS MAC (Message Authentication Code) Optional
Short-distance (ITS-G5)
TLS secured end-to-end session packet for IP based communication

Figure 3. Structure of a C-ITS message suitable for short-range and long-range communication (adapted from C-ITS Security & Governance 2023, 12).

The protocols required for a short-range communication and their headers are shown in the innermost red section in Figure 3 (ETSI Security Envelope) and in the GeoNet Basic Header section for packet routing located outside the ETSI Security Envelope.

In short-distance communication, the message contains four different elements: (1) C-ITS message (DENM, IVIM, etc.) according to C-Roads Platform specifications, (2) a header field according to the BTP (Basic Transport Protocol) (OSI-4, transport layer), (3) GeoNetworking protocol header fields that implement packet routing (OSI-3, network layer), and (4) a signature field intended for ensuring the integrity of the message and the confidentiality of the sender. Once a message has been generated using the fields on these protocol layers, it is ready to be sent to the data link (OSI-2, data link layer) which is ITS-G5 in short-range communication according to C-Roads Platform.

The C-ITS message fields described above are used to ensure the routing, confidentiality and integrity of messages in short-range communication environments. The message types defined by C-Roads Platform are used in the messages and the routing of messages to the correct recipients and applications is ensured using the GeoNetworking and BTP protocols. The sender’s confidentiality and message integrity are ensured by message signatures implemented using certificates in accordance with EU CCMS.

IP-network-based communication requires, in addition to the header fields in the above protocols, protocols running on that network. The Advanced Message Queuing Protocol (AMQP) was presented earlier in Section 6.2.3 as part of the introduction of long-range communication. It is an open and lightweight protocol specifically developed for IoT applications that operates at the application level (OSI-7) of the OSI model. The protocol manages message queues, signing, and retransmission to ensure the reception of messages. It is designed for large, distributed systems.

In long-range communication, connections between devices are encrypted for each session using the Transport Layer Security (TLS) protocol version 1.3. This is described in more detail in Section 6.3.3. Table 11 below summarises the C-ITS message header fields, their purpose and the standards that specify them.

Table 11. Description of the protocol header fields used in C-ITS messages.

Component	Definition	Purpose	Specified in
ETSI Security Envelope			
SignerID and Signature	Verification of the privacy of the sender and the integrity of the message	**SignerID** is an identifier that links the message sender to their public key certificate. It allows the recipient to find and use the correct public key and ensures the confidentiality of the sender. **Signature** is a cryptographic message signature that verifies the integrity of the message. It is created with the sender's private key and the recipient can check the integrity of the message content with a public key.	ETSI TS 103 097
DENM / IVIM / SPATEM / MAPEM…	Message content	The actual data content of the C-ITS message.	C-Roads Platform profile specifications
BTP	Basic Transport Protocol	Transport layer protocol used for long-range communication between vehicles and infrastructure. BTP is lighter and more efficient than TCP or UDP (User Datagram Protocol). Like UDP, it is designed for connectionless, low latency and high-performance communication. It particularly works together with the GeoNetworking protocol.	ETSI EN 302 636
GeoNet Ext. Header	GeoNetworking protocol	An extended header field in the GeoNetworking protocol that provides additional information for routing a message based on geographic locations. This header contains additional fields and metadata needed for optimized routing and processing of messages between vehicles and infrastructure.	ETSI EN 302 636

Component	Definition	Purpose	Specified in
GeoNet Common Header	GeoNetworking protocol	GeoNet Common Header is a basic header contained by all messages in the GeoNetworking protocol. It contains the general information necessary for processing and routing the message. GeoNet Common Header is a common component to which other GeoNet Extended Headers can be added, depending on message needs and application.	ETSI EN 302 636
C-ITS message for short-range communication (ITS-G5)			
GeoNet Basic Header	GeoNetworking protocol	GeoNet Basic Header is the minimum core component in any GeoNetworking message. It contains critical information necessary for the basic routing and processing of the message. Additional Extended Headers may be attached to it if additional information is needed to route or process the message.	ETSI EN 302 636
TLS 1.3 session packet for IP-based communication, TLS end-to-end			
End-to-end Application Properties	Messaging protocol	AMQP (Advanced Message Queuing Protocol) is a separate message-delivery protocol that can be used in back-end systems in particular but is not part of the basic C-ITS communication protocols covered by ETSI standards. However, the role of AMQP in IP-based C-ITS solutions is described in the C-Roads Platform C-ITS IP Based Interface Profile Version 2.0.8. AMQP is an open, freely available communication protocol used to relay messages between back-end systems that require high communication scalability and reliability.	ISO/IEC 19464:2014 and OASIS AMQP 1.0 Specification
TLS Header	Transportation layer (OSI-4) security	TLS Header refers to the header of the TLS encryption protocol used to encrypt an unencrypted C-ITS message inside the ETSI security envelope for communication over IP networks. C-Roads Platform requires the use of TLS version 1.3. TLS provides encryption, message integrity checking and authentication, which is used in the IP network for communication between servers and systems.	RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3
TLS MAC, optional	Checking message integrity	Transport Layer Security Message Authentication Code. Part of the TLS protocol, used to check the integrity of the message by the recipient.	

6.3.2 Signing a C-ITS message

The station generating and sending a C-ITS message digitally signs the message in accordance with the EU CCMS, using its own private key. The sender’s signature is located inside the ETSI security envelope of the C-ITS message in the SignerID & Signature field (Figure 3). The recipient uses the information in the field to check the sender’s confidentiality and integrity of the message using the sender’s public key. At this stage, the content of the message is not encrypted (the content itself does not contain confidential information), but the digital signature ensures that the sender is trusted (authenticity) and that the content of the message has not altered in transit (integrity).

Different mathematical algorithms can be used to generate a digital signature, of which the RSA (Rivest-Shamir-Adleman), introduced in 1978, is probably the most well-known and widely used. It was the first to present a Public Key Infrastructure (PKI) based encryption algorithm adopted in use based on the factoring problem of large prime numbers[1]. The digital signature is one of the most significant innovations in public key cryptography, and the first standard related to it was published in 1991 (Digital Signature Standard, DSS, ISO/IEC 9796). (Menezes, van Oorschot, Vanstone 1996, 2)

RSA is still very widely used and integrated into several encryption standards (e.g. SSL encryption, electronic signature, email encryption, VPNs). However, in recent times, the more efficient ECDSAs (Elliptic Curve Digital Signature Algorithm) have become significantly more common, especially in applications that require high-speed message encryption. The new algorithms are based on solving a mathematically different problem (discrete logarithmic problem, so-called elliptic-curve cryptography), which means that the algorithm works with significantly shorter encryption keys. This, in turn, improves message processing speed and reduces delay.

For all used encryption algorithms, it should be noted that signing messages is a more mathematically demanding procedure than checking the authenticity and integrity of the message. (Menezes, van Oorschot, Vanstone 1996, 11)

The currently used PKI encryption algorithms are generally considered highly secure. However, it is generally recognised that future quantum computers are threatening the protection provided by current encryption algorithms, and as a result, encryption algorithms are constantly being developed (Post-Quantum Cryptography, PQC). An example of this is the project launched by the US National Institute of Standards and Technology (NIST) in 2015 to standardise PQC algorithms. The project is carried out by the Computer Security Resource Center (CSRC), which was the first to publish PQC standards in late 2024 (Federal Information Processing Standards, FIPS 203-205).

[1] The factoring problem is a one-way function based on the idea that multiplying two large prime numbers is easy, but finding the original prime factors from their product is extremely difficult. Because of its mathematical background, PKI encryption is also commonly called asymmetric encryption.

The PKI algorithms[1] used by the European C-ITS system are described in the European Commission's C-ITS Certificate Policy 2024, (70–73). In addition to the algorithms used, the Certificate Policy also includes requirements for the used key length and requirements for the secure storing of keys.

The C-ITS Certificate Policy specifies that encryption keys must be stored in cryptographic Hardware Security Modules (HSM). HSMs are dedicated devices specifically designed to securely store and manage encryption keys. HSMs are typically used in applications requiring high security, such as payment systems, electronic document signatures and healthcare systems. The modules also include security features against potential digital and physical tampering attempts.

High-performance HSM modules are devices optimized for message signing and are capable of performing a significant number of signature operations per second. One example is the French company Thales, one of the world's leading companies in digital cyber and information security solutions. Its HSM modules (Thales Luna HSM 790) are capable of performing signature operations based on faster ECDSA algorithms at a rate of 20,000 operations per second – equivalent to approximately 1.7 billion per day. (Thales Luna HSMs, n.d.)

In large-scale C-ITS implementation, the daily number of C-ITS messages can reach up to several billions[2]. This must be taken into account in the capacity of devices used in signing and forwarding messages in the system. This may require specific technical implementations for encryption keys and signature operations, such as scaling computing capacity or optimising the technical design of the C-ITS system. These measures help ensure that the signing of the messages does not, in the worst case, paralyse the functioning of the C-ITS system as service deployment scales up.

The use of HSM modules as a part of C-ITS stations is based on the requirements set out in the European Commission's C-ITS Certificate Policy document. According to the policy, the assessment of the security level of the C-ITS station (ISO 15408, Common Criteria) must include validation of the security level of the HSM intended for key management (see Section 4.1.3 in this study). However, this requirement is targeted at assessing the level of security of roadside and vehicle C-ITS stations. Similar definitions have not yet been determined for manufacturing central C-ITS stations.

[1] C-ITS systems use fast ECDSA_nitP256_with_SHA 256 and ECDSA_brainpoolIP256r1_with_SHA 256 algorithms based on elliptic curve cryptography to sign messages, as well as the ECDSA_brainpoolip384r1_with_SHA 384 algorithm with a longer encryption key to ensure the integrity of the ECTL list (specified in more detail in ETSI TS 103 097)

[2] In late 2024, the Dutch C-ITS ecosystem (also known by the working title "Talking Traffic") received more than 1.5 billion C-ITS messages per day via the central C-ITS stations. More than half of the traffic light crossings in the country are connected to the system and it is also used to implement a wide range of C-ITS services, such as traffic light crossing services, emergency vehicle priority and approach warning services and roadworks warnings (Monotch interview 2024).

To sign messages, solutions are available that leverage either the servers' own computing capacity or cloud services, where key storage and the signing process are managed programmatically by software designed for this purpose. There is a general perception that HSMs are the most secure way to implement features related to PKI keys, whereas server and cloud-based solutions offer more scalable and cheaper solutions in terms of performance.

The lack of clarity regarding the use of HSMs has led to differing opinions on the necessity of using HSMs in the processing of PKI keys in central C-ITS stations. Some feel that the use of HSM modules is necessary, while others find that the use of HSM modules is unnecessary in data centre solutions with high physical security. It would be important for the European Commission to clarify this requirement as it has a significant impact on the cost management of the central C-ITS stations' computing capacity and PKI signatures.

6.3.3 Session-specific encryption

Communication between central C-ITS stations operating over IP networks in C-ITS service implementations must be encrypted on a per-session basis. The requirements related to this operation are defined in the C-Roads Platform specification describing the requirements for IP-based communication (C-ITS IP Based Interface Profile 2023, 51–53).

Session-specific encryption must be based on the TLS protocol, which is commonly used on the Internet and operates at the transport layer (OSI Layer 4) to secure data transmission. The primary function of the TLS protocol is to establish a secure connection between two communicating parties.

TLS is a protocol standardised by the Internet Engineering Task Force (IETF), an open organisation focused on standards and protocols related to Internet. The latest version 1.3 of the protocol was defined in the organisation's RFC document 8446 in 2018, whose use is also required by C-Roads Platform (IETF RFC 8446 2018). One of the best-known applications of TLS is the secure HTTPS connection provided by web browsers, which uses TLS technology to implement encryption.

C-Roads Platform requires that authentication and message encryption in communication based on the TLS protocol use X.509 certificates, as defined in the IETF RFC 5280 document (IETF RFC 5280, 2008). The X.509 standard, which defines certificate management and structures, is part of the ISO/IEC 9594 standard series ("Directory Services"). Certificates compliant with this standard are commonly used in network security, identity and access management, and electronic signatures.

The implementation of security for the back-end systems of long-range communication solutions defined by C-Roads Platform follows the standard session-based security used in the public Internet. As in public Internet communication using the TLS protocol, the connection between parties begins with agreeing on the encryption protocol, during which encryption keys are exchanged. Authentication is based on X.509 certificates, which ensure that the parties are communicating with a trusted entity. After this, the communication is encrypted according to the TLS protocol.

In a C-ITS system based on the EU CCMS, session-based security, as described above, is used for connections between back-end systems over the IP network. In addition, each C-ITS message sent between central C-ITS stations is digitally signed using the sender's private key, allowing the recipient to verify that the message comes from a trusted source. This procedure is performed regardless of whether the message is transmitted via a short-range radio network or over an IP-based long-range communication.

TLS and X.509 provide strong security for communication between central C-ITS stations. Additionally, the digital signature for each transmitted message based on the PKI architecture of the EU CCMS, ensures that even if an attacker manages to access the TLS-protected channel, they cannot alter the messages without the recipient detecting it during the message signature verification.

6.4 Central C-ITS station system load management

Central C-ITS stations in large-scale C-ITS deployments must process significant volumes of C-ITS messages. This processing includes message generation and signing procedures, as well as verifying the integrity and authenticity of received and forwarded C-ITS messages (signature verification).

The number of messages processed by a central C-ITS station increases as the variety of services it provides grows and as more C-ITS stations send messages to it. The loading caused by C-ITS message signing on central C-ITS stations can be approached from a variety of perspectives. This section examines the load on central C-ITS stations in more detail and highlights methods for managing this load.

6.4.1 Services to be deployed

Different C-ITS services load central C-ITS stations in different ways due to the characteristics of the services and their implementations. The differences in services are particularly reflected in the frequency of updates to C-ITS messages related to each service. ETSI defines the technical operation of various C-ITS services in a two-part standard series ETSI EN 302 637[1].

According to ETSI, depending on the speed of the vehicle, a single vehicle can send 1–10 Cooperative Awareness Messages (CAM) per second (ETSI EN 302 637-2 2019, 17–18). Meanwhile, some other messages are sent considerably less frequently. For example, vehicles only send Decentralized Environmental Notification Messages (DENMs) when detecting a critical event. ETSI does not precisely define the frequency of message submission after the detection of the event, as this depends on the nature, duration and severity of the event (ETSI EN 302 637-3 2019, 25–26).

[1] ETSI 302 637 defines CAM and Part Two defines DENM services. CAMs (Cooperative Awareness Message) contain e.g. vehicle position, direction and speed data. DENMs (Decentralized Environmental Notification Messages) can be used to communicate versatile data about various traffic and road network disruptions, such as slippery sections on the road, emergency braking of vehicles or obstacles on the road.

Traffic lights may transmit Signal Phase and Timing (SPAT) messages to approaching vehicles 1–10 times per second. As the transmission frequency is not specified precisely in the ETSI standards, the speed of the delivery of service messages depends on the configurations of the traffic signal controller.

In other words, the services to be deployed and their implementation methods have a significant impact on the volume of messages in C-ITS service implementations.

6.4.2 Number of users

The more users C-ITS services gain, the greater the volume of C-ITS messages circulating in the network. In first-phase long-range communication solutions, the message flow is mainly from central C-ITS stations to end users, who access the services with applications installed on mobile devices. Vehicles do not generate any CAM or DENM messages; instead, all service messages are created by the central C-ITS stations that provide services for mobile applications installed on end users' smartphones.

Later, when in-vehicle C-ITS stations become more common, they can generate significant amounts of data (CAM/DENM), exchange this data with each other, and send the same data to the central stations. In the central C-ITS stations, these messages can be relayed to vehicles as well as available for use by systems outside C-ITS service implementations.

It should also be noted that the implementation method of C-ITS services will significantly influence the routing of vehicles' CAM and DENM messages in the future.

If C-ITS services are implemented solely using a long-range communication solution and integrated C-ITS stations in vehicles, CAM and DENM messages may primarily be transmitted only to the car manufacturers' central C-ITS stations via mobile networks. However, if the architecture of the C-ITS service implementation is using a hybrid or short-range communication solution, the CAM and DENM messages can also be transmitted to the roadside C-ITS stations through short-range communication and from there to the national central C-ITS stations. In the hybrid solution, the messages generated and forwarded by vehicles can be sent both to the car manufacturer via the mobile network and to the national central C-ITS station via roadside C-ITS stations.

6.4.3 Structure of C-ITS service implementation architecture

The architectural implementation of C-ITS services have a significant impact on the signature operations performed by central stations. A national C-ITS service implementation may be based on a single central C-ITS station, through which all messages between infrastructure and vehicles pass.

By contrast, a higher number of central stations can be implemented to distribute also the signature operations. For example, one unit could serve the main road network, and one for each larger city. Smaller towns and cities could implement their own C-ITS communications through a joint central C-ITS station procurement or by using the services provided by an existing central C-ITS station.

On the other hand, the roles of central C-ITS stations could also be divided according to the services they provide. Some basic services could be provided from a single national central station and city-specific services could be provided through the cities’ own central stations. Central stations could also be given different roles related to specific tasks: Formation of C-ITS messages using input data from outside the C-ITS implementation architecture, transmission of C-ITS messages between regional C-ITS service implementations, and provision of C-ITS end-user services.

6.4.4 Management of signing entities

Structural measures related to the architecture of the C-ITS service implementation can also be used to manage the locations where C-ITS messages are signed. If the aim is to reduce the number of measures related to signing in central C-ITS stations, several services can be implemented using separate vehicle C-ITS stations or roadside equipment capable of signing C-ITS messages (stations supporting hybrid communication). For example, limited vehicle groups (emergency vehicles, public transport) can be equipped with separately installed vehicle stations, in which case the vehicle C-ITS stations can be used to sign C-ITS messages. Similarly, roadworks sites could be required to be equipped with roadside C-ITS stations, which would enable roadworks to transmit signed roadworks warnings to the central station.

As previously noted in Section 6.3.2 on C-ITS messages signing, the verification procedure for received C-ITS messages is computationally less demanding than the signing process of C-ITS messages. Therefore, managing signing points can also help control the load on central C-ITS stations.

6.4.5 Number of signatures and load to central C-ITS stations

As shown in the previously presented options related to C-ITS service architectures (Sections 6.4.1–6.4.4), there are various ways to control the number of C-ITS message signing operations handled by central C-ITS stations. Therefore, the number of signatures performed by a single central C-ITS station is stongly depends on the services deployed, the number of users, the technical implementation of the C-ITS architecture, and national requirements - such as whether data is relayed via C-ITS vehicle or roadside stations, or by utilizing data from the National Access Point (NAP).

Due to the factors mentioned above, it is very challenging to assess the total load caused by the number of messages in different situations. The Dutch C-ITS ecosystem serves as the best point of comparison for the number of messages processed in the network. This ecosystem is based on a single national central C-ITS station that relays messages between infrastructure and vehicles, currently processing over 1.5 billion messages per day. End users access C-ITS services through central C-ITS station and mobile applications provided by private sector service providers. The Dutch ecosystem also offers services for professional transport services, such as the prioritisation of emergency vehicles at traffic light-controlled intersections and warnings related to roadworks. In the Netherlands, more than half of traffic light-controlled intersections (approx. 1,500) are connected to the system.

The Dutch example is a good benchmark for the future C-ITS ecosystem in Finland, as the number of traffic lights in both countries is roughly comparable, and services in Finland will probably rely significantly on long-range communication solutions. However, the Dutch comparison is primarily relevant in terms of the volume of messages transmitted. The development of the Dutch C-ITS system began in 2016 in the Talking Traffic development project, which introduced its own national technical implementations. For example, in the Dutch model, central stations do not at the moment sign messages according to the C-Roads Platform specifications or the EU CCMS methods.

6.4.6 Central C-ITS station message load management

This section discusses the methods used for the load management of central C-ITS stations and evaluates the load generated by C-ITS service implementations from the perspective of the central C-ITS station. It begins with a rough estimate of the potential load the C-ITS system could impose on its central station, considering both the number of messages and the resulting network traffic.

Message number and PKI operations

The current scale of the Dutch C-ITS implementation could represent the scope and level of the Finnish C-ITS system in a few years. This is likely around the year 2030, assuming the C-ITS is implemented in accordance with C-Roads Platform requirements. It is assumed that, similar to the Netherlands, the Finnish C-ITS system would be largely based on a single national central C-ITS station, and all PKI operations carried out in separate HSM modules. HSM modules currently on the market could handle the signature load caused by C-ITS messages (the performance of the reference device mentioned in Section 6.3.2 is approximately 1.7 billion PKI signatures per day, 20,000 operations per second). Two HSM modules would probably be needed, as the volume of C-ITS messages varies according to traffic, being higher during the day and lower at night. Redundancy of operations would also make sense in terms of risk management in the system.

As C-Roads Platform specifications regarding the processing of PKI signatures in central stations are still underway, there is not yet knowledge of whether the implementation of central stations will require an HSM. If the signatures were implemented based on of the servers' own computing power or HSM cloud services, the capacity would be even more likely to be sufficient to manage the message load.

Required telecommunications capacity

It can also be useful to estimate the load caused by message traffic on the central C-ITS station using traditional communication capacity metrics. The calculation below is based on the assumption that all message traffic is routed through a single point and estimated to be 500–800 bytes of the average C-ITS packet according to C-Roads Platform.

The estimated size of the C-ITS package is based on a pilot project previously carried out in Finland, in which the size of the SPAT message signed in a short-range communication solution was 509 bytes (Kynsijärvi et al. 2024, 46). To this, the headers of the protocols used in the long-range IP network communication (AMQP, TLS 1.3, TCP and IP) have been added, estimated to total approximately

140–280 bytes. The 800-byte packet size is used in the calculation. The size of messages may vary significantly depending on the message type.

As a second basis for the calculation, the previously presented Dutch reference system is used, in which the national centralised C-ITS station currently processes more than 1.5 billion messages per day. For the calculation, a slightly higher number of messages, two billion messages per day, is used.

Based on the above baseline assumptions, the required network capacity for a central C-ITS station would be approximately 150 Mbit/a[1] in each direction. Taking into account variations in traffic volume at different times of the day and their impact on the number of C-ITS packets, it can be estimated that the required network capacity (inbound/outbound) required by the central station would vary between 50 and 300 Mbps (the load generated by the signature is about 15% of this, roughly 80 to 140 bytes per message).

As a conclusion, it can be noted that this represents a significant volume of traffic, but it does not require any special arrangements. The result indicates the data communication capacity required by the central C-ITS station based on the assumptions of the calculation (e.g., the bandwidth needed for the cloud service in which the central C-ITS station is hosted).

Managing information processing capacity

The central C-ITS station can manage the load generated by signature functions in a variety of ways. One of these is the previously mentioned design of the C-ITS service architecture, which provides various options for central C-ITS station system load management. This approach can be considered as a traditional form of horizontal scaling of computing capacity, where servers are added to the system through the structural network development and the roles given to central stations. The same type of scaling is also represented by the duplication of individual servers and the use of load balancing.

Another way of implementing capacity scaling in central stations involves increasing the capacity of a single server (memory, processor power, etc.) in line with vertical scaling principles. Cloud service providers offer the optimal conditions for scaling by enabling dynamic vertical scaling, allowing capacity to be adjusted as needed.

[1] The objective of the calculation is to obtain the demand for telecommunications capacity X Mbit/s. In a day, 2,000,000,000 packages of 0.8 kilobytes pass the central point → 1,600,000,000 kilobytes. This multiplied by eight gives the number of kilobits: 12,800,000,000 Kbit = 12,800,000 Mbits. The number of seconds in a day is 86,400 (60*60*24). The required capacity is 12,800,000 Mbps / 86,400 s = 148.15 Mbps.

6.4.7 Conclusions

Despite the structural implementation of the C-ITS architecture, central C-ITS stations must process significant volumes of C-ITS messages. The number of messages increases as the number of services and users increases, and as more vehicles are equipped with integrated C-ITS stations.

When assessing the scope of the future Finnish C-ITS system in this chapter, the used point of comparison was the Dutch C-ITS ecosystem, where currently more than 1.5 billion messages are transmitted daily at the national level. The laod estimation was based on assumption of two billion C-ITS messages per day and an estimated average C-ITS message size of 800 bytes. This is estimated to be a realistic reflection of the Finnish C-ITS system in the early 2030s.

Calculations based on baseline assumptions indicate that the number of messages would correspond to an approximate bandwidth requirement of 150 Mbps. Taking into account variations in traffic volume during different times of the day, the bandwidth requirement is estimated to range between approximately 50 and 300 Mbps.

If the national architecture is based on a single central C-ITS station, the above-described figures represent the bidirectional data capacity required specifically for national central C-ITS station, for example, located in a cloud service or a data centre. It is important to emphasize that this capacity requirement does *not* refer to the general bandwidth needs of the communications networks used by the C-ITS service implementation in general, but solely to the bandwidth required by the central C-ITS station. As a conclusion regarding bandwidth needs, it was pointed out that capacity requirement may be significant, it does not cause problems in terms of network connectivity or general performance of servers.

Section 6.3.2 also assessed the computational load caused by the C-ITS message signing operations for a central C-ITS station in a national centralized architecture. The conclusion noted that two modern HSM units would suffice to sign the messages used in the calculation scenario (2 billion messages per day). As a reference, the Thales Luna S790 HSM module (Thales Luna HSMs, n.d.) was used. This module is capable of performing approximately 20,000 signature operations per second using the PKI algorithms defined by C-Roads Platform (ECDSA and the 256-bit RSA key used for signature). This translates to an average of 1.7 billion signing operations per day.

If the C-Roads Platform profile specifications or the C-ITS security and certificate policy do not require the use of a hardware-based HSM units, the estimated number of signing operations can be handled using cloud service providers' HSM services or server-based software solutions.

Regarding the load caused by the signing requirements, it was noted that even though the number of messages will be significantly higher in the long-range communication solution, and in particular the model based on the national central C-ITS station, signing the message volumes estimated for the future scenario at reasonable costs would be feasible already with the technologies available today.

Taking into account the expansion of C-ITS service implementations and the continuous growth in message volumes, along with the ongoing continuous advancements in technology and computing capacities, as well as the various technical and architectural approaches related to C-ITS service implementation presented in this chapter, it can be concluded that central C-ITS stations based on long-range communication have good preconditions for coping with the load they are exposed to.

The assessment of the adequacy of the communications bandwidth in the implementation of the central C-ITS station does not address more broadly on the suitability of public communications networks operating without quality-of-service guarantees in long-range communication solutions. This perspective is discussed separately in Chapter 0 of this study.

6.5 Example of the implementation of the national C-ITS system

This section presents a fictitious example of a national C-ITS system in line with the previously presented requirements and the C-Roads Platform architecture. The example is not a recommendation for the national implementation of the C-ITS system. Instead, it describes the possible architecture for the implementation of C-ITS services, demonstrates the operation of central C-ITS stations, the end-user interfaces of C-ITS services, the role of vehicles, and the use of various source data channels.

Figure 4 illustrates a hypothetical example of a national C-ITS service implementation architecture operating based on one national central C-ITS station, in addition to which one city has also introduced its own city-specific central C-ITS station. In the example, the role of these two central stations is to generate C-ITS messages based on various input data sources. In both C-ITS service implementations, end-user services are delivered via central C-ITS stations and mobile applications provided by service providers (provider-specific protocol implementations are used between the service provider's central station and the mobile application, see Figure 2, p. 59).

The solution shown in the example is in line with the principles of the long-range communication solution described in Section 6.2.3. Its technical implementation does not utilise any roadside C-ITS stations, nor does the provision of end-user services rely on vehicle C-ITS stations that support cellular network technology. In the example, the city-specific emergency vehicle priority service at signalized intersections is implemented using C-ITS on-board units (OBUs) that support mobile network technology. The connections between the central C-ITS stations shown in the figure allow the city's C-ITS service implementation to make use of the services provided by the national central station (and vice versa). In this example, the central C-ITS stations communicate with each other according to the principles of the EU CCMS and share the available C-ITS message types with each other. The example solution does not take a stand on how the central C-ITS stations or end-user mobile applications have been implemented (by a public or private operator).

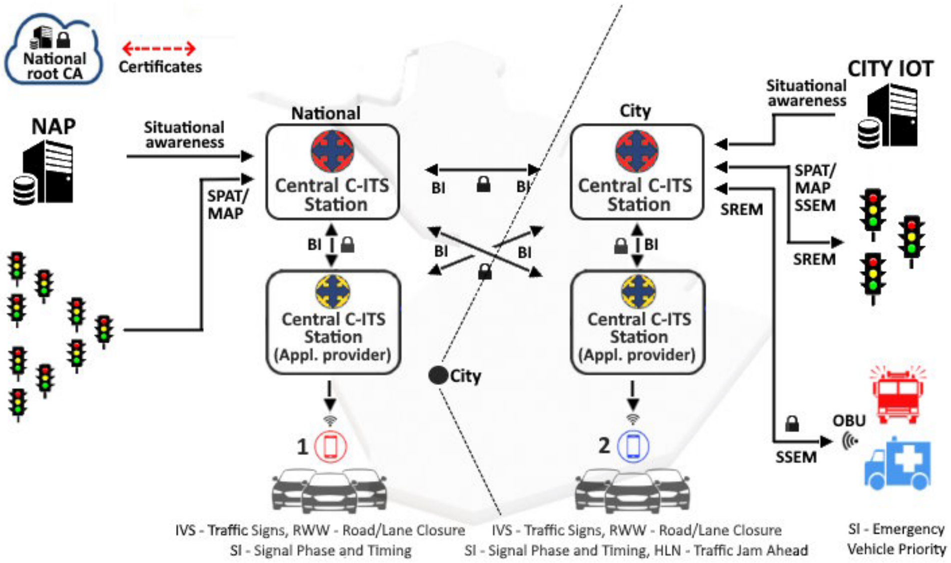

National root CA
Certificates
NAP
Situational awareness
SPAT/ MAP
National
Central C-ITS Station
BI
Central C-ITS Station (Appl. provider)
1
BI
BI
BI
BI
City
City
Central C-ITS Station
BI
Central C-ITS Station (Appl. provider)
2
CITY IOT
Situational awareness
SPAT/ MAP SSEM
SREM
SREM
OBU
SSEM
IVS - Traffic Signs, RWW - Road/Lane Closure
SI - Signal Phase and Timing
IVS - Traffic Signs, RWW - Road/Lane Closure
SI - Signal Phase and Timing, HLN - Traffic Jam Ahead
SI - Emergency Vehicle Priority

Figure 4. An imaginary example of a Finnish C-ITS system based on a long-range communication solution and central C-ITS station.

In the example implementation, the national central C-ITS station provides the following C-ITS services to road network users.

(1) The central C-ITS station retrieves the status information and impact areas of fixed and dynamic traffic signs through the National Access Point (NAP). Based on this information, it provides C-Roads-compliant Traffic Signs IVS service (In-Vehicle Signage), which conveys the current valid state of traffic signs through its own mobile application (C-ITS application 1).

(2) From the same source, the national central C-ITS stations also obtains location data of roadworks due to the enforcement of the SRTI and RTTI regulations and the ongoing development of the National Contact Point (NAP). Using this data, the national central C-ITS station generates warning messages for roadworks and provides C-ITS warning messages for road-users when approaching roadworks (Road Works Warning - Road/Lane Closure service).

(3) In the example, the national central C-ITS station is also connected to traffic signal controller units owned by Fintraffic Road Ltd and cities, which provide the central station with status information for the traffic signal group and forecasts for the timing of the next signal phase change (SPAT, MAP). Based on these, the central C-ITS station offers the Signal Phase and Timing service belonging to the Signalized Intersection (SI) service category to road users.

In the example, a city-specific central C-ITS station offers more diverse C-ITS services for those moving around in the city area than road-users using the national central C-ITS station. This is enabled by the increasingly common Smart City IoT solutions deployed in cities. The city’s IoT solution produces a real-time situational awareness of traffic in the city, which allows the example system to deliver a traffic jam warning service (Traffic Jam Ahead) to drivers moving within the urban area. Additionally, in the example, emergency vehicle traffic signal priority is implemented locally in the city through separate C-ITS On-Board Units (OBUs) installed on emergency vehicles. In the priority system, the OBUs transmit Signal Request Extension Messages (SREMs) via the city-operated central C-ITS station to the traffic lights, which acknowledge the requests with Signal Request Status Extension Messages (SSEMs).

In the example, connections between central C-ITS stations allow the city's C-ITS mobile application 2 to provide the same national services as the mobile application 1. It offers all nationally implemented services both inside and outside the city area, but in the city area, it also provides a Traffic Jam Ahead service, which is part of the Hazardous Location Notification (HLN) service category including the above-mentioned traffic congestion warning in the urban area. The national central C-ITS station could transmit warning messages of approaching queue tails in the urban area to mobile application 1. However, example C-ITS application 1 does not include the support of this Traffic Jam Ahead service.

The example of mobile applications described above shows that the C-ITS service provider decides which services it will implement in its own C-ITS mobile application. This applies not only to mobile applications but also to C-ITS OBUs integrated into vehicles. The same applies to the actual implementation of C-ITS services, i.e. the visual implementation of the service presented to the end user. In its requirements, C-Roads Platform does not specify this level of detail for implementation. C-Roads Platform defines the C-ITS messages used to implement the services in one specification (C-Roads C-ITS Message Profiles 2023) and the use cases of the implementation of C-ITS services in another (C-Roads C-ITS Service and Use Case Definitions 2024).

The emergency vehicle priority in traffic lights shown in the example is based on the hybrid vehicle C-ITS stations installed in vehicles (separate installation). According to Figure 4, the stations use the mobile network to request priority from traffic signal controllers connected to the city's central C-ITS system using signed signal request extended messages (SREM), as defined by the C-Roads Platform. The controllers respond with a signal request extended message (SSEM) indicating whether the request has been granted.

The national implementation example in Figure 4 is implemented according to the architecture defined by C-Roads Platform. In the example, central C-ITS stations and OBUs installed in emergency vehicles obtain the PKI keys required for signing messages from the national root certificate authority. Using these credentials, the EU CCMS trust domain governs communication on the connections marked with a lock symbol, i.e. in the links between the central C-ITS stations and the city-level central C-ITS station and emergency vehicles. Other connections shown in Figure 4, such as retrieval of external data inputs from sources like the NAP and City IoT systems, and communication between central C-ITS stations and mobile applications, are not managed under the EU CCMS trust domain. For these connections, responsible parties for operational administration of the central stations ensure the security of the solution.

In the example implementation in Figure 4, the responsibility for collecting input data lies with both central C-ITS station operators (national C-ITS operator and the city-level operator). They are responsible for the confidentiality and integrity of the data they process. In the example, these entities can be classified as providers of essential transport services and are therefore subject to the information security requirements set forth by the NIS1 and NIS2 Directives. In the example, C-ITS services are provided by these central C-ITS station operators (see Figure 4, Appl. provider), and their information security management must comply with a certified information security management system in accordance with ISO 27001. Additionally, all C-ITS station operators in Figure 4 are subject to the requirements of the C-ITS Security Policy published by the European Commission. This policy mandates continuous assessment of security risks related to the generation and processing of C-ITS messages, as well as the protection of personal data in service implementation. The same obligations also apply to the emergency authority, which in the example serves as the operator of the C-ITS OBUs installed in emergency vehicles.

7 Requirements and feasibility of the interchange server

7.1 Interchange server

Interchange servers are an essential part of the pan-European architecture of C-ITS service implementations based on the C-ITS trust model. These servers are not part of the C-ITS trust domain but have a specific role in enabling communication between national C-ITS service implementations - including the networks operated by road operators and service providers - in C-ITS solutions based on long-range communication.

No requirements have been set for the implementation or operational management of interchange servers in the C-ITS security or certificate policy documents, and their information security is not managed in accordance with the EU C-ITS Security Credential Management System (EU CCMS).

The role of interchange servers and their integration into networks based on the C-ITS trust model, as well as communication between interchange servers, information security and the management model, are described in the C-Roads Platform specification C-ITS IP Based Interface Profile (2024). The specifications and requirements concerning the interchange server presented in this chapter are primarily based on this C-Roads Platform specification.

7.2 Interchange servers as part of the architecture of C-ITS implementations

Interchange servers interconnect national and regional C-ITS service implementations and relay traffic between them. At the regional level, they aggregate C-ITS service implementations operated by the road authorities at the state and cities, as well as by vehicle manufacturers and private service providers. At the national level, they enable communication between C-ITS service implementations across different countries.

From the perspective of network technology, communication between interchange servers takes place in IP-based network environments, such as the public Internet or closed IP-based wide area networks (WANs) operated by service providers. The C-Roads Platform specifications do not define or restrict the use of these networks, including aspects of the network architecture, such as whether an open or closed IP network is used.

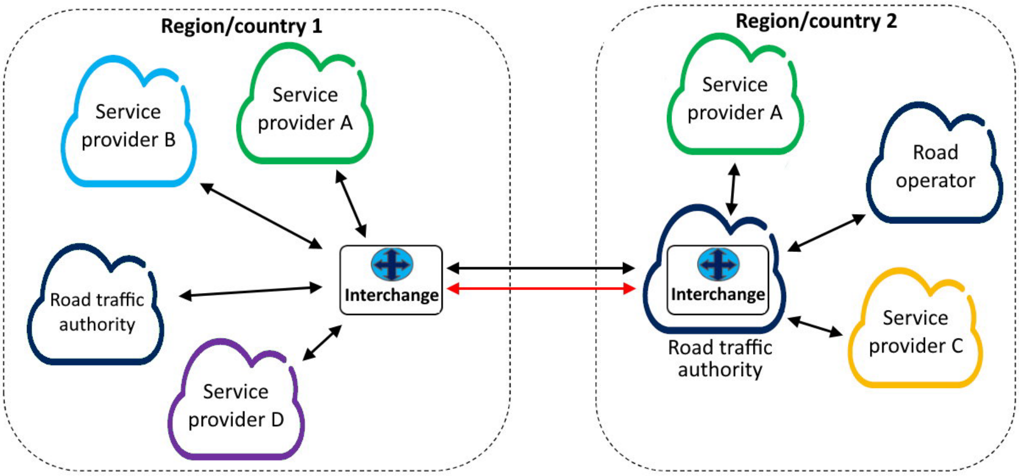


Figure 5. The role of interchange servers in the exchange of information between national and regional C-ITS service implementations (adapted by C-ITS IP Based Interface Profile 2023, 32).

C-Roads Platform does not precisely define the number of interchange servers used in regional implementation or their relationship with central C-ITS stations. Figure 6 presents possible network architecture models for the interaction between C-ITS service implementations and interchange servers.

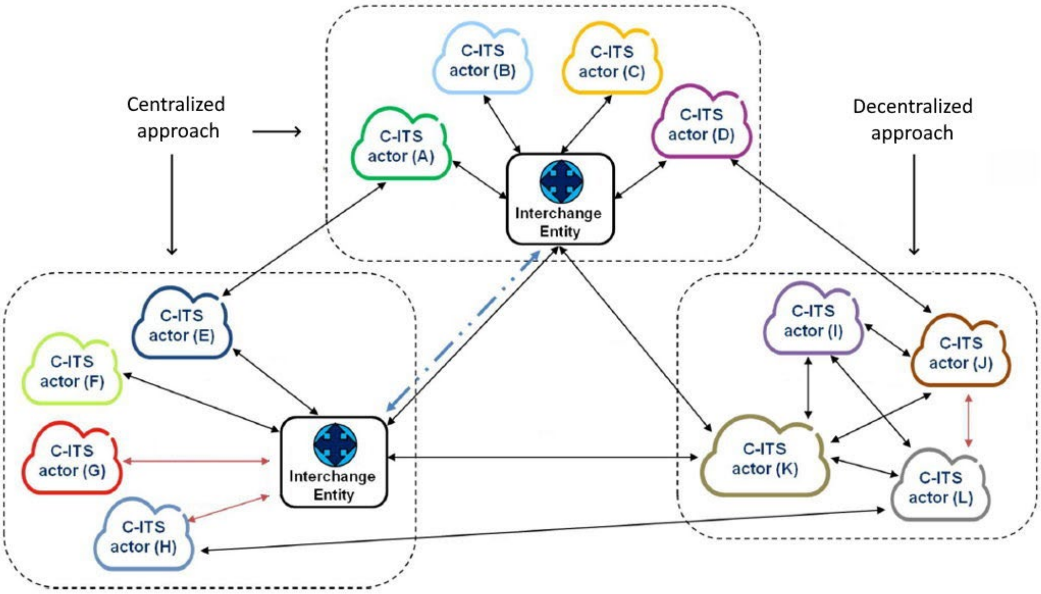


Figure 6. Different networking structures between interchange servers and regional C-ITS service implementations (C-ITS Actor in the Figure; adapted by C-ITS IP Based Interface Profile 2023, 57).

The architecture diagram in Figure 6, illustrating the structural alternatives involving C-ITS Actors[1] and interchange servers in regional C-ITS service implementations, demonstrates the flexibility of the model defined by the C-Roads Platform in enabling communication between regional and national C-ITS service implementations.

Each C-ITS service implementation can have a distinct architecture. The decentralized approach in Figure 6 demonstrates that intercommunication between multiple C-ITS service implementations does not necessarily require an interchange server in this approach, all C-ITS service implementations communicate directly with each other, enabling data exchange across all regions. In the centralized approach, the structure is based on traditional star topology, where the central C-ITS stations do not communicate directly with each other. Instead, all inter-domain communication is routed through an interchange server. However, the star topology does not prohibit direct point-to-point links between certain C-ITS service implementations as exemplified by the A↔E connection in Figure 6).

[1] The C-ITS Actor is a group of organisations or individuals involved in the operation of the C-ITS system that have specific roles in the operation of the system and its use cases. For example, the actors may be organisations implementing the operation of C-ITS or processing C-ITS data, such as road operators or C-ITS station operators. C-ITS actors may also be users of the C-ITS system. The roles, responsibilities and actors related to the operation of C-ITS are defined in ISO Standard 17427-1. (ISO 17427-1 2018)

7.3 Interchange server communications

Interchange server communications refers to both the communications between the interchange servers themselves and the communication between interchange servers and the central C-ITS stations of regional C-ITS implementations, as illustrated in Figure 6 of the previous section.

This section focuses on describing the requirements of C-Roads Platform related to the communication and information security of interchange servers. (C-ITS IP Based Interface Profile 2023, 32–51)

7.3.1 Communication protocols

The C-Roads Platform defines three protocols for communication with interchange servers: BI (Basic Interface), II (Improved Interface) and the ISO-standardised AMQP protocol (ISO/IEC 19464). The BI and AMQP protocols were already introduced in the previous Chapter 6, which covers central C-ITS stations.

The Improved Interface protocol (II) is an extension between interchange servers that provides a dynamic control layer on top of the BI protocol. It enables automatic discovery of national and regional C-ITS services or data sources behind the interchange servers. This protocol eliminates the need for manual configuration of services within each C-ITS domain. As a result, it creates a scalable and dynamically operating system for a Europe-wide C-ITS service implementation consisting of multiple administrative domains.

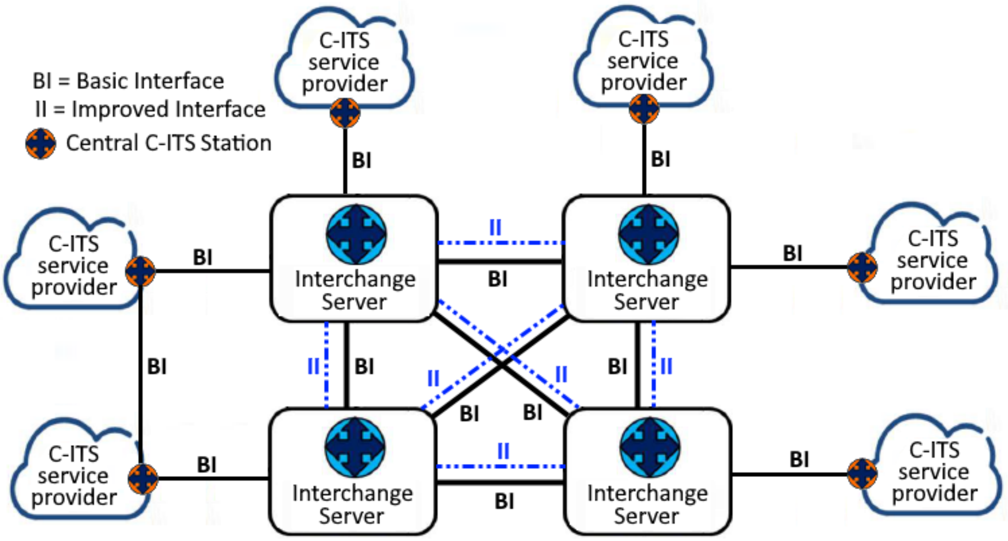


Figure 7. Example of a network of back-end systems, central C-ITS stations and interchange servers operating behind C-ITS solutions based on long-range communication, and protocols operating between the systems.

<u>Technical operational description of protocol II</u>

To ensure a functional network of interchange services, the specification requires that each registered server must establish a control channel to other active interchange servers using the Improved Interface protocol. This protocol enables query-based communication between the interchange servers. Through these queries, the C-ITS services and data sources connected to each interchange server can be automatically discovered, and related subscription can be made.

This allows automatic forwarding of C-ITS services between regional implementations in different countries, forming a Europe-wide C-ITS service architecture.

The control channels between interchange servers are established using a commonly agreed subscription procedure. In this procedure, an interchange server requests information from another server in order to establish a data exchange channel. The response includes the endpoint details of the remote server, such as address and port information, which are required to set up the channel.

As part of their continuous operation, interchange servers actively maintain information about the C-ITS services provided by other servers and notify peers of any changes to their own services. They receive subscriptions related to C-ITS services from other interchange servers and automatically forward subscription originating from C-ITS central units within their own network. C-ITS services refer to C-ITS service messages related to specific geographical areas that are provided by each interchange server.

The address and port information required to establish a control channel between interchange is available from a dedicated DNS registry[1], which contains the necessary details for the control channel. These DNS registries are maintained within a DNS service operated by a governing authority specifically for C-ITS service implementations.

It is the responsibility of the interchange server operator to keep the DNS registry information up to date. Interchange servers must also update their own data information about other active servers and their DNS records at least once every 12 hours. The operation of the DNS system as part of the network of interchange servers is described in more detail in Section 7.5.

The establishment of the Improved Interface control channel is based on the HTTPS protocol secured by a TLS certificates. For security reasons, the connection should not be allowed if the initiator’s information is not found in the DNS records. The requirements related to TLS certificates are described in Section 6.3.3 of this report.

An interchange server must either be capable of reading and maintaining information about the C-ITS services provided by other servers and offering this information to its connected central C-ITS stations, or be able to redirect C-ITS station queries to other interchange servers (redirect policy). The status of this redirect capability is maintained in the metadata of the interchange servers. If an interchange server declares this capability as mandatory in its own metadata, the connected servers must implement the same functionality.

[1] Domain Name System (DNS) is a name service system that operates on the Internet or other IP networks. It maintains information about the IP addresses and names of computers and services on the network. The operation of the system is based on documents RFC 1034 and 1035 specified by the Internet Engineering Task Force (IETF).

It is also important to note that support for the Improved Interface (II) is an optional feature for an interchange server (C-ITS IP Based Profile 2024, 33). If a server implements support for the interface, it must meet the requirements defined by C-Roads Platform. Without II support, the role of the interchange server is limited, and only certain functions may be used based on bilateral agreements between interchange servers.

7.3.2 Communication encryption

Section 6.3.1 discussed the structure of C-ITS messages, i.e. the protocol header layers used in communication. As described in that section, a C-ITS message transmitted over an IP network essentially consists of two parts: (1) the part used in short-range communication, which contains the essential information for the actual C-ITS message - such as the C-ITS message type, location data related to the sender or receiver (provided by the GeoNetworking protocol), and the actual C-ITS message - and (2) the protocol header fields used in IP-based communication.

The security of long-range communication is implemented on two layers. The first layer involves message signing according to EU CCMS using a PKI method (Figure 8, ETSI Security Envelope). By signing the messages, the integrity of the data inside the ETSI security envelope and the authenticity of the sender are ensured. The sender signs the data within the envelope using its private PKI key (Figure 8, SignerID & Signature field), and the message recipient verifies that the data has not altered in transit by checking the sender’s public key and signature.

In an IP-based network, central C-ITS stations and interchange servers add an AMQP protocol-compliant header field outside the original signed ETSI security envelope (Figure 8 AMQP header field). This header contains routing and filtering information derived from the data within theETSI security envelope. The most important elements include the type of original C-ITS message and its associated geographical location, encoded using the so-called QuadTree data structure[1]. With this information, the interchange server does not need to process the contents of the ETSI security envelope, allowing it to filter and route messages using the header field of the AMQP protocol only. The interchange server also does not verify the message signature.

The second security layer in IP-based communication is implemented through sessions between back-end servers. The ETSI security envelope and AMQP header field form the final message, which is encrypted for transmission between back-end systems using the TLS encryption protocol. The encrypted message is then transferred over TCP/IP protocols. The receiving server decrypts the message and can perform routing and filtering operations based on metadata fields defined in the AMQP protocol.

[1] Quadtree is a tree data structure commonly used in spatial data systems in which each internal node has exactly four children. It is used to repeatedly divide a two-dimensional space (computer screen or map) into four quadrants or regions. This data structure was named a quadtree by Raphael Finkel and J.L Bentley in 1974.

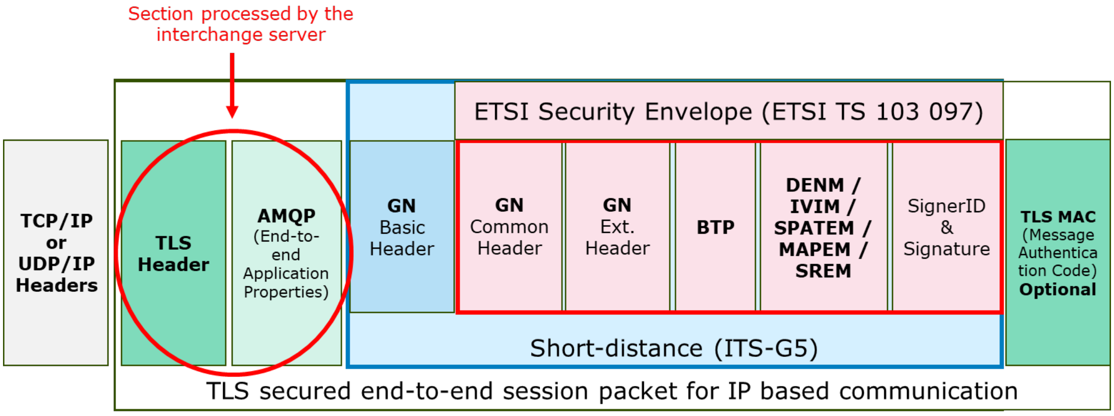

Section processed by the interchange server
ETSI Security Envelope (ETSI TS 103 097)
TCP/IP or UDP/IP Headers
TLS Header
AMQP (End-to-end Application Properties)
GN Basic Header
GN Common Header
GN Ext. Header
BTP
DENM / IVIM / SPATEM / MAPEM / SREM
SignerID & Signature
TLS MAC (Message Authentication Code) Optional
Short-distance (ITS-G5)
TLS secured end-to-end session packet for IP based communication

Figure 8. The figure shows the packet section used by the interchange server in long-range communication (adapted from C-ITS Security & Governance 2023, 12).

7.3.3 Scaling the transmission capacity

The C-Roads Platform defines the message flow handling feature knows as "sharding" in Annex G of the C-ITS IP Based Interface Profile C-ITS specification.

The sharding feature enables the distributed processing of large message flows by allowing C-ITS messages to be optimally divided among a predefined number of forwarding units After distributed processing, the messages can be reassembled in the correct order. Enhancing forwarding capacity through multiple forwarding units is referred to as horizontal scaling. An alternative method for scaling the forwarding performance would involve improving the processing power of a single interchange server which is known as vertical scaling.

Interchange servers within the C-ITS system that use multiple forwarding units for processing messages indicate the use of the sharding feature to others via the Improved interface protocol (by setting shardCount > 1). This allows sending C-ITS stations to split the outgoing data stream based on the number of processing units on the receiving server. The packets are divided, marked accordingly, and given sequence numbers. On the receiving side, the packets are distributed across multiple units (load balancing) and reassembled into the correct order after processing.

7.3.4 Session-level trust domains

Figure 9 illustrates the session-based trust domains related to the connections between the back-end systems used in C-ITS service implementations. The figure categorizes the trust domains into three different areas.

(1) The red line represents the session-based trust domain, which operates according to the C-Roads Platform specifications for session security. It uses TLS 1.3 encryption protocol and X.509 certificates as defined by C-Roads Platform.

(2) The orange line represents the trust domain according to the EU CCMS, where central C-ITS stations sign or verify messages based on signatures. Sessions are also encrypted within this domain using the TLS protocol; however, not all units support the C-Roads Platform specified method (indicated by the green outline).

(3) The green dashed line indicates a country-specific C-ITS domain that does not support the same TLS standard or X.509 certificate version defined by C-Roads

Platform but still implements the ETSI security envelope procedure according to the EU CCMS.

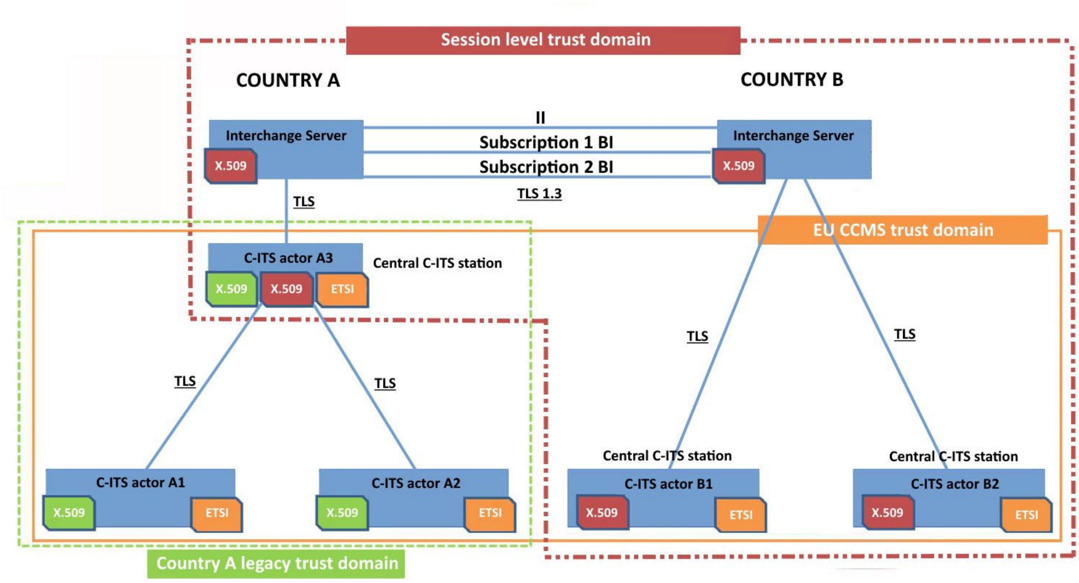


Figure 9. Trust domains of the back-end communications used in the EU CCMS and long-range communication solutions (C-ITS IP Based Interface Profile 2023, 63).

7.4 Operational management of interchange servers

The C-Roads Platform does not directly define requirements for the operational management of interchange server in the same way that the European Commission’s security and certificate policies do for the operational management of central C-ITS stations (see Chapter 4).

Different requirements apply for the operational management of interchange servers and central C-ITS stations due to their different roles within the C-ITS system. Central C-ITS stations generate and sign C-ITS messages, which places responsibility on their operators for the reliability of the underlying data used in the C-ITS messages as well as for related security threats. Additionally, central C-ITS station operators are responsible for managing the PKI keys used for signing. To ensure secure management of these activities, the C-ITS security policy requires operators of C-ITS stations to maintain a certified information security management system in accordance with ISO 27001. In contrast, interchange servers neither generate nor sign C-ITS messages, nor do they manage the associated PKI keys. Due to these differences, operators of interchange servers are not required to maintain a comparable certified information security management system.

Although interchange servers are not subject to the same requirements as central C-ITS stations, they form an essential part of the future C-ITS system and its pan-European operation. The European Cybersecurity Directive classifies the transport sector as a critical sector, meaning that actors operating within it (e.g., road operators, municipalities, and large private organisations) are subject to the requirements of NIS2 Directive. Based on this classification, the operational management of interchange servers can be considered to fall under the scope of the NIS2 Directive (EU 2022/2555 2022 and EU 2010/20/EU 2010)[1]

7.5 Governance model for the network of interchange servers

Section 7.2 (Interchange server communications) discussed the security requirements related to the communication of interchange servers. In accordance with the section, the TLS security protocol and X.509 certificates – commonly used in Internet communications - that are part of regular Internet use are used to secure the connections between interchange servers.

In addition to the security solutions described above (Sections 7.3 and 7.4), the communication between interchange servers and the back-end systems of long-range communication-based C-ITS service implementations makes use of the DNS (Domain Name System), which is commonly used in Internet communications.

However, the session-based security model and DNS system defined by the C-Roads Platform specifications do not rely on available Certificate Authorities or DNS services on the public Internet. Instead, C-Roads Platform defines a dedicated governance model for the use of these services within the operation of C-ITS back-end systems. The key components and functions of this governance model are illustrated in Figure 10.

[1] Annex 1 of the NIS2 Directive includes traffic management control operators as well as the operators of intelligent transport systems as defined in Article 4, point (1), of the ITS Directive 2010/40/EU among the sectors of high criticality. The ITS Directive defines intelligent transport systems as, for example, systems that apply information and communication technologies in the field of road transport.

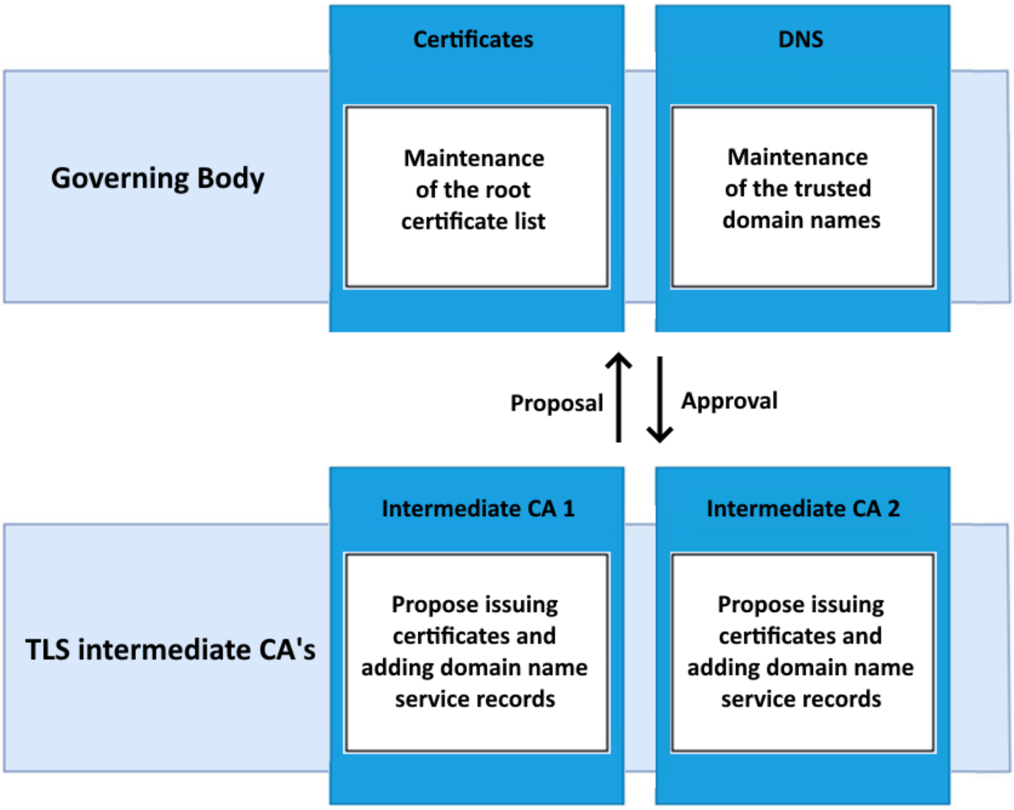

Governing Body
Certificates
Maintenance of the root certificate list
DNS
Maintenance of the trusted domain names
Proposal
Approval
TLS intermediate CA's
Intermediate CA 1
Propose issuing certificates and adding domain name service records
Intermediate CA 2
Propose issuing certificates and adding domain name service records

Figure 10. The figure shows the actors in the C-Roads Platform governance model and their relationships (C-ITS IP Based Interface Profile 2023, 63).

The governance model is based on the operations of a specifically established ‘Governing Body’. This governing body is responsible for managing and operating the TLS root certificate service and administering the trusted DNS server used for interchange server communication (e.g., adding and deleting DNS records).

The governing body is the highest authority within the governance model and is responsible for the following tasks:

- Management of TLS root certificates (Root CA)
- Approval of TLS intermediate CA
- Administration of DNS records for trusted domains
- Approval of interchange units to the trusted domain list based on recommendations of intermediate CAs
- Trusted domain list maintenance
- Publication of revoked certificates.

Similarly, TLS intermediate CAs are responsible for:

- Approve C-ITS actors and propose issuing TLS certificates to the governing body
- Propose adding an interchange server or central C-ITS station to trusted domain DNS records maintained by the governing body.

The C-Roads Platform do not define a specific procedure or model for the appointment of governance model entities or the formation of the governing body. Broadly speaking, it can be assumed that the establishment of a pan-European governing body will likely fall under the responsibility of the Commission, the Certification Policy Authority (CPA). The actors at the TLS intermediate CA level are national or regional authorities responsible for proposing central C-ITS stations and interchange servers emerging within their respective areas for inclusion in the governance model structure.

7.6 Interchange servers' network effects in C-ITS

This section discusses the benefits of deploying interchange servers in the implementation of C-ITS services. The benefits are examined from the perspective of the network effects enabled by interchange servers. These network effects are assessed from three different perspectives.

- Improved availability to end-users
- Promoting the technological neutrality of different service implementations
- Ease of implementation of C-ITS services

All of these aspects contribute to facilitating the deployment of C-ITS services while simultaneously enhancing the availability of C-ITS services to end-users. For these reasons, they can be expected to contribute effectively the widespread adoption of C-ITS services across new service domains and implementations throughout Europe.

Previously, network effects have only been studied in research focusing on short-range communication, which aimed to examine the impact of increasing the use of vehicle C-ITS stations on the availability of C-ITS services. In practice, the aim of the work was to determine by means of a conditional probability analysis, how likely it is that a vehicle equipped with an C-ITS station can receive a C-ITS message based on vehicle-to-vehicle communication as the penetration rate of vehicle C-ITS stations increases. (Öörni 2024)

In this section, the network effects of interchange servers are examined separately in two different operating environments: (1) interchange servers as a part of the national C-ITS service deployments and (2) interchange servers as a part of the pan-European C-ITS service deployments.

7.6.1 Interchange servers as a part of the national architecture for C-ITS service implementations

The potential role of the interchange server in national C-ITS service deployments is to act as an interconnection point between regional C-ITS service deployments. Previously, section 7.2 described various network structures between regional C-ITS service deployments (see Figure 6, p. 84). Figure 6 shows that C-Roads Platform does not define a detailed networking model between regional C-ITS service deployments. Based on the networking models shown, the central C-ITS stations in C-ITS services can communicate directly with each other (a "decentralised model") or with each other via a single interchange server (a "centralised model"). Both approaches enable the same functionality, i.e. C-ITS messages can be exchanged between C-ITS service deployments. These two options are further illustrated in Figure 11 below.

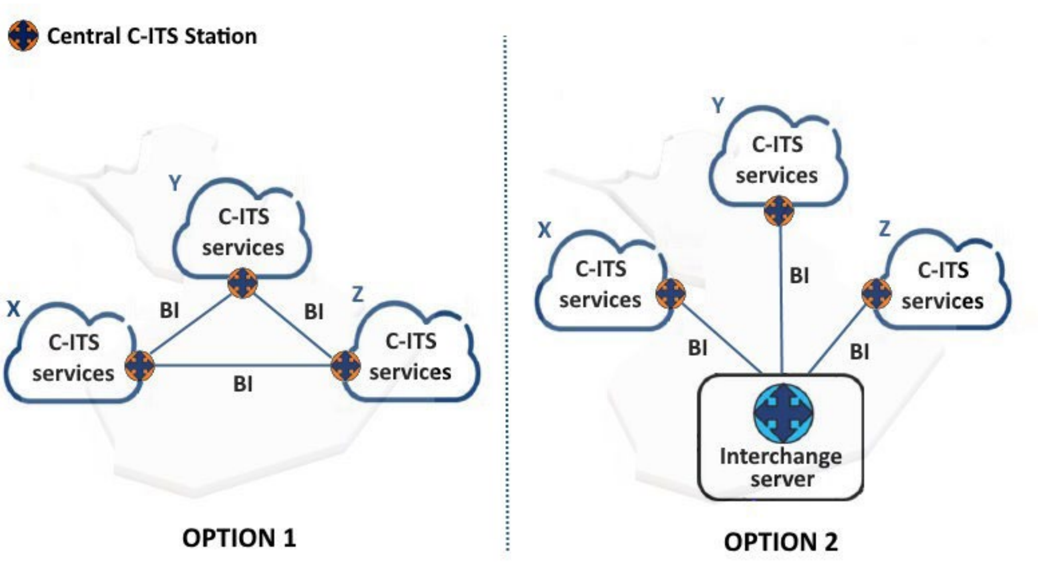


Figure 11. Illustration of the role of the interchange server in the example of a national architecture for C-ITS services.

Below is an assessment of the network effects produced by the interchange server, based on the previously presented perspectives of analysis.

Improved availability to end-users

The options illustrated in Figure 11 show that both network architectures enable the transmission of C-ITS messages between different service areas. In practice, this means that C-ITS services implemented in each service area (X, Y, Z) can be provided to end users across all service areas. Based on this, it can be concluded that in such a national deployment, the interchange server does not specifically enhance the network effects related to end-user accessibility. The same effects can also be achieved by interconnecting the central C-ITS stations or the service areas.

Promoting technological neutrality

The conclusion presented in the previous paragraph also applies to the promotion of technological neutrality. In both options shown in Figure 11, each C-ITS service deployment can be realised using different communication methods (short- or long-range) and messages can be transmitted either via direct links between central C-ITS stations of the service deployments or centrally via interchange server. As a result, both solutions equally promote the technological neutrality of C-ITS services.

Easier implementation of C-ITS services

As regards the ease of the implementation of C-ITS services, the interchange server can be expected to have a positive impact. Figure 11 also clearly illustrates this perspective. In option 2, a single C-ITS service deployment can reach all the other deployments through just one link between a central station and the interchange server. The higher the number of separate C-ITS Services in the national C-ITS architecture, the greater the impact of this characteristic.

7.6.2 *Interchange servers as a part of the European architecture for C-ITS service implementations*

In this section, the role of the interchange server is examined as a part of a pan-European C-ITS architecture. An example of the pan-European C-ITS architecture is presented in Figure 12 below.

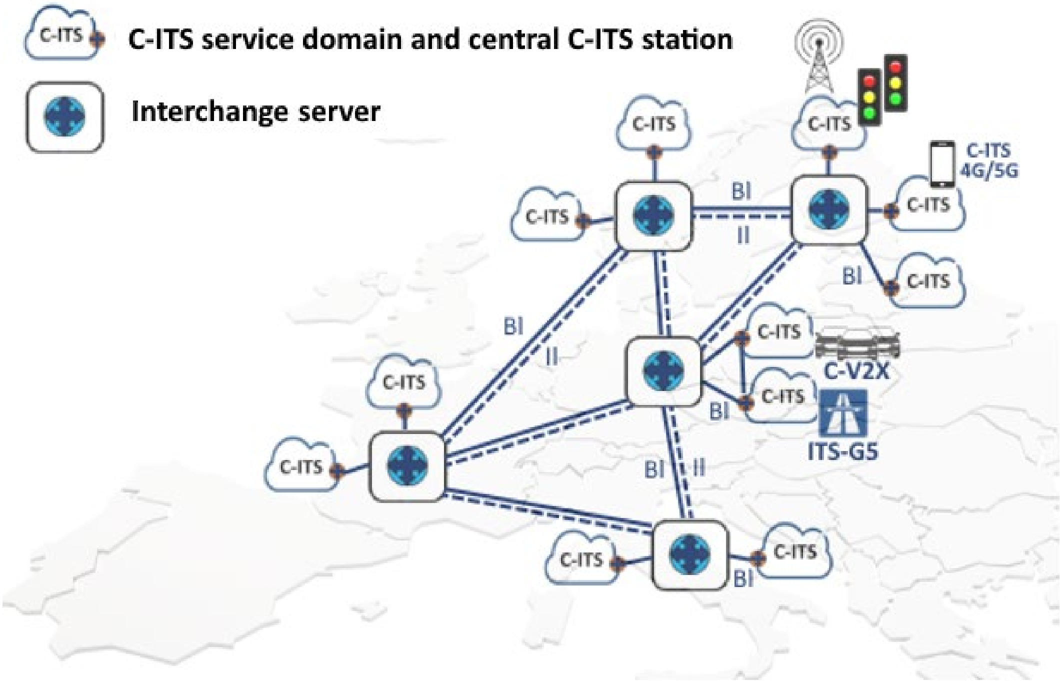


Figure 12. Interchange servers as a part of the common European C-ITS architecture.

Figure 12 illustrates the interchange servers joining the C-ITS services implemented in the pan-European C-ITS architecture, along with interchange servers that connect these regional deployments. The figure also includes examples of C-ITS service deployments using different technologies. For Finland, a long-range C-ITS deployment based on cellular network technologies is shown, with traffic lights connected at the national level and services accessed through mobile applications. In Central Europe, a C-ITS service deployment marked with vehicles represents a fleet from a single car manufacturer equipped with C-ITS onboard stations supporting C-V2X technology. The Central European C-ITS service deployment marked with a motorway symbol describes the services carried out by a local road operator using ITS-G5 technology, covering a nationwide motorway network.

In the example architecture shown in Figure 12, the C-ITS deployment has expanded into a unified European C-ITS architecture. It forms a network of interchange servers and central C-ITS stations that comply with the requirements of the C-Roads Platform and EU CCMS, enabling the exchange of C-ITS messages between service areas. In theory, connections between different C-ITS service areas could also be established using the model presented in Figure 11, by directly linking each central C-ITS station to each other's. However, at the practical level, this approach is no longer feasible in such a large-scale C-ITS architecture. The use of Improved Interface protocol (II), enabled by interchange servers, is also an essential part of the operation of the pan-European C-ITS architecture. It enables interchange servers to advertise C-ITS services to each other, automatically sharing information about new C-ITS services introduced in various areas. This significantly simplifies the maintenance and efficient operation of C-ITS deployments.

The network effects produced by interchange servers are assessed below as part of the common European C-ITS architecture as shown in Figure 12.

Improved availability to end-users

The improved availability to end-users is examined using the examples in Figure 12.

Example 1

In the example shown in Figure 12, vehicles equipped with C-V2X technology and associated with the car manufacturer’s C-ITS service area can utilise the C-ITS services implemented in Finland based on long-range communication and the local road operator’s C-ITS services based on ITS-G5. For example, C-ITS messages transmitted from traffic lights can be relayed via the local central C-ITS station and Finnish interchange servers to the car manufacturer’s central C-ITS station. This enables the provision of traffic light-related C-ITS services to the vehicles. The same can also be accomplished by a local road operator. In that case, the messages can be transmitted via roadside stations supporting ITS-G5 technology to the road operator's central C-ITS station, from where they can be transmitted via the interchange server and the car manufacturer’s central C-ITS station to OBUs supporting C-V2X technology. In the example in Figure 12, a direct link between central C-ITS stations has also been implemented to support inter-service are communication.

Example 2

Finnish C-ITS end users using a mobile application can receive messages such as roadworks warnings when driving within the C-ITS service area of a motorway in central Europe. The warning messages can be transmitted via C-ITS roadside units (RSUs) installed along the motorway to the local road authority’s central C-ITS station. From there, the messages are relayed via interchange servers to the central C-ITS station of the Finnish C-ITS service provider and from there delivered to the C-ITS application on the road users' mobile device.

As the examples show, the interchange server plays an important role in promoting availability to the end-users of the European C-ITS system.

Promoting technological neutrality

Referring to the previous examples, interchange servers often enable the use of regional C-ITS services even when end-users are using different technologies than those deployed in the C-ITS service area in which the vehicles are physically located.

However, interchange servers do not provide a solution to all possible C-ITS communication methods. The example solution does not enable direct communication between vehicles equipped with different technologies, although in many cases, this can be facilitated via a central C-ITS station and interchange servers. However, in relation to vehicle-to-vehicle communication, this report does not consider whether all Vehicle-to-Vehicle (V2V) services can operate through C-ITS back-end systems with sufficient speed. One example is the Emergency Brake Light (EBL) data transmitted between vehicles.

In the example, reaching vehicles equipped with ITS-G5 technology would be the most difficult (not shown in the figure). They could only be reached in C-ITS service domains with roadside C-ITS stations that support the same technology.

As a conclusion, it can be noted that although C-ITS service domains could be partly joined through connections between central C-ITS stations, interchange servers significantly promote technology neutrality in the common European C-ITS architecture.

Easier implementation of C-ITS services

Interchange servers are not useful for the implementation of internal services within a single C-ITS service area. However, connecting the central C-ITS station of the service area to the nearest interchange server makes it possible to disseminate the services of the service domain to nearly all service users across Europe. At the same time, interchange servers make it significantly easier for the C-ITS service domain to become part of the pan-European C-ITS architecture.

In summary, it can be stated that interchange servers significantly contribute to the easier implementation of C-ITS services.

7.6.3 Summary

The network effects of interchange servers were examined in the previous sections in two different contexts: interchange servers as a part of the national and pan-European C-ITS architectures.

Based on the examination presented in Section 7.6.1, the interchange servers produce some positive network effects in the national example architecture (Figure 11, p. 94). In particular, interchange servers promote the interconnection of national C-ITS services, thus facilitating the implementation of communication between service areas. This positive impact will gain emphasis as the number of C-ITS service areas in the national implementation increases.

Section 7.6.2 discussed the role of interchange servers as part of a unified C-ITS architecture in line with the requirements of C-Roads Platform and EU CCMS. In the section, it was recognised that the interchange servers play an important role in promoting the availability of C-ITS services and accessibility to their end-users. At the same time, they promote the technological neutrality of C-ITS service domains and the ease of implementation of C-ITS services.

7.7 Models for the procurement of interchange servers

Typical procurement models related to IT systems have been identified in the context of acquiring interchange servers. These models are not described in the standards or C-Roads Platform specifications, nor there are any specific requirements related to them that would differ from public procurement legislation.

This section presents four different approaches to the procurement of an interchange server: community-driven open source development, custom implementation, custom implementation based on open source software, and commercial product procurement. These descriptions are not yet recommendations for the Finnish model, but they rather outline how the models function and highlight general perspectives related to each approach.

7.7.1 Community-driven open source development

This subsection discusses the community-driven open source development approach to software solutions development. The content of the subsection is largely based on an expert interview with the COSS association (The Finnish Centre for Open Systems and Solutions; COSS ry interview 2024), which promotes the use of open source and open technologies in both the private and public sectors in Finland. Another key source used in this section is the study conducted by the European Commission in 2021 on the impacts of open source code on Europe’s technological self-sufficiency, competitiveness and innovation capabilities (Blind et al. 2021) and the expertise in the working group.

EU and open source

The European Union’s Open Source Strategy 2020–2023 encourages the adoption of open source solutions. The vision is to encourage the sharing and reuse of software solutions, knowledge and expertise to achieve better returns on software development efforts. Although the strategy formally ended in 2023, practical support for open source software has continued. The aim remains of further strengthening the Union’s digital autonomy, promoting transparency and enhancing technological development and cooperation.

The EU has also outlined the use of open source code as one way of promoting the digital sovereignty of the EU. In 2021, the EU carried out a study with the specific objective of examining how open source code promotes technological independence, competitiveness and innovation in the EU. Based on studies, the EU recommends increasing the use of open source code in public administration, which can help reduce the total cost of ownership, avoid vendor lock-in and improve digital sovereignty.

The key observations of the research work are described below.

- Technological independence: open source code reduces dependence on foreign suppliers.
- Competitiveness: open source code promotes competition and reduces barriers to entry.
- Innovation: open source code enables faster innovation by enabling companies and developers to utilise and build on existing solutions.

According to the report, the contribution of open source code to the European Union’s GDP is considerable. Open source code is expected to generate up to EUR 100 billion in added value for the EU economy in the coming years if investments increase. (Blind et al. 2021)

Open source utilisation models

Open source development is a broad concept. It may mean using open source code in your own in-house development or sharing your own source code openly. It may mean using a solution made by a private person or a product solution maintained by a large organisation that has been made available as an open source code in your own development. The utilisation can be straightforward use of open source code, or the implementation of your solution as a part of an open source community.

Foundation-based governance

Foundation-based governance is one key method for implementing open source maintenance and management. Examples of foundation-based governance include Eclipse Org, Linux Foundation and Apache Foundation. Foundation-based governance seeks to also look for funding providers from private sector operators that could benefit from the created solution. A typical feature of the solutions funded with a foundation basis is their generic nature, which makes it possible to utilise the solution as widely and independently as possible.

Community-based governance

A community can also be built around open source development where members are committed to developing the solution further. Members typically also finance the development and community activities. It is also possible to apply for external funding for the activities if the solution can be demonstrated to produce extensive benefits for the development of business life and various sectors.

Regardless of whether the open source is governed by foundation-based or community-based governance principles, the support measures provided by the model for the development of the solution and for the members of the development community are essential added value. Indeed, in an open source code, support measures distinguish private publications from community-based or foundation-based solution development, which typically have a sound governance base.

The support measures include the following tasks:

- Developer community’s support for each participating entity.
- Technical ecosystem development community support (technical development environment with version management).
- Agreeing on common governance models (project management principles, procedures that contribute to maintaining quality control standards).
- Quality control processes.
- Intellectual property rights and license management.
- Ensuring long-term support and maintenance for the product.

Funding is essential for an open source solution when the solution is implemented using a community-based model and the aim is to achieve a long-term, reliable solution. Many open-source organisations and communities aim to produce value-added services in addition to free implementation as funding mechanisms, such as consultation, add-ons, SaaS services, training and certifications. (COSS ry interview 2024)

Companies also often make use of open source products as a key part of their own products. As a result, companies' business activities may significantly rely on the open source solution. In these operations, companies seek to actively participate in the community so that they can influence decision-making and development priorities and receive community support for the utilisation of source code (risk management).

Sometimes companies set up their own open source communities. In this case, they may make the software of some key services or products or especially some parts of them openly available. When the solution is opened up for others, the aim is to create an active development community around it, which accelerates the development of the solution while producing new innovations. Naturally, the company itself continues to play a strong role in the activities of the open community, which provides it with good visibility into the directions the development is taking and is able to manage them.

In the situations described above (participation in or establishment of an open source community), the activities should be based on a carefully considered open source utilisation strategy. The company uses the strategy to define precisely what kind of benefits it strives to achieve, which open code licences it will use and which it will avoid. The company also uses the strategy to ensure the business benefits of this activity and to identify how it improves competitiveness. This may be achieved by opening up some core technologies for the development of an open source community, while preserving the critical layers of added business value on top of the technologies. (Linux Foundation 2024)

Custom implementation

Custom software is generally developed and designed for a specific company, organisation or purpose. Unlike ready-made product solutions intended for general use, custom software accurately meets the customer's specific requirements and needs. It is often built from scratch or it is developed using existing software components to perfectly fit the user's processes, objectives and operating environment. As a rule, the custom implementation model provides the organisation with strong control over the copyrights and code of the software.

The custom solution is built to accurately meet the processes and requirements of the specific organisation. Usually, it is based on a specific need that does not match the exact needs that many organisations have. The custom implementation model is often not used in situations where the solution under development is strongly defined and standardised. In such situations, companies would be more likely to use market-based product solutions or use an open source community model for co-creation.

The aim of the interchange server is to establish uniform requirements and functionalities at the European level, making a custom solution appear less suitable. However, the operation of the interchange server and support for different functions are the same for everyone. In addition, the interchange server does not need to be integrated locally into different data interfaces. Instead, its communications are always based on pre-determined methods with other interchange servers or central C-ITS stations. On the other hand, if clear national customisation needs are identified for the interchange server, to which ready-made products or solutions cannot respond, customisation can bring organisation-specific benefits.

7.7.2 *Open source-based custom implementation*

A common method currently used for developing a custom solution involves the use of open source code in the development work, if this is enabled by the licensing used in the open source code. This model is commonly referred to as “forking” in open source communities. It involves copying the source code of an open-source project to create a separate, independent development branch.

There may be many different motives for using open source code in a custom implementation.

This may involve a private operator launching the work to create a product solution and identifying an open source community related to the topic that is developing a solution that resembles the operator’s product or offers at least some ready-made parts for it. In these situations, the use of open source code is usually motivated by financial benefits. The open code offered may significantly accelerate the development time of the product and may also provide benefits in the further development and lifecycle management of the product. The part of a company’s own product that is implemented using open source code may develop “by itself” by the open source community, which creates new features for it, ensures its security or always updates it to meet new requirements (e.g. standards).

This activity also involves the risk mentioned in the previous section. If an organisation bases its solution on an open source solution code available at a given moment and does not intend to actively participate in the community, it takes the risk. In such a case, the organisation would lack visibility into open source development and related decision-making and would not benefit from community support for issues identified in the open code. Active participation in the development of an open source community also ensures that the organisation has the necessary expertise in the utilised source code. The magnitude of these risks varies greatly depending on the maturity of the utilised open source community and the solutions it creates.

The above factors lead to another example of “forking”, i.e. the utilisation of existing source code. In this example, the organisation identifies an open source community that is useful for a product it is developing and integrates (part of) a solution developed by the community into its work to develop its own solution. The organisation uses the community’s solution as a basis of the development of, for example, a commercial product and starts developing business layers necessary to stand out in the market. However, at the same time, the organisation is involved in the activities of the open community whose solution it utilises in its product to affect how the work will develop and also ensure it has sufficient competence to make use of it.

The third example involves a community member who is initially strongly involved in developing a shared solution with the community, but later, as the work progresses, chooses to build their own version based on the community’s implementation. This decision may be due to differing views within the community on the direction in which the solution is developed or the needs identified by a member of the community that are not in line with the views of the other members of the community. If the organisation no longer continues to be involved in the open community’s activities, the risks presented above will materialise: the organisation will no longer have visibility into community activities and can no longer influence them or receive the support of the members of the community. However, even in this model, cooperation with the original source code maintainer may still be possible. The organisation may continue as a member of the community if, in addition to its own development branch, it also commits to the community’s rules, development forks and investments.

There are examples of successful forking as described above, such as the LibreOffice, which was forked from OpenOffice, and is now a more active and commonly used version. This was also the case with io.js, which was originally forked from Node.js, but later merged into a Node.js project.

7.7.3 Product procurement

A product-based software solution can be a faster, less expensive and more stable alternative for organisations that do not need custom solutions that meet their special needs. Product procurement includes ready-made updates, extensive support and documentation, and scalability, making it an attractive choice.

The downside of product-based solutions is that they do not always meet all specific needs. They may restrict customisation possibilities, create supplier dependency and lead to unnecessary features or increased costs for additional features.

Product-based solutions available as ready-made commercial software are often cheaper in total cost than custom software implementations. The deployment of product-based solutions tends to be significantly more affordable, even if the solutions include site-specific customisation, for example, related to product localisation or integration of surrounding data sources and systems.

Deployment is usually followed by service fees during the contract period. Compared to custom implementation, service fees involve significantly better predictability for the financial management of the solution. Typically, service fees include the necessary security updates to the product. Updates also typically include necessary changes resulting from updates made to standards.

If the buyer organisation wishes to develop the product-based solution according to its specific interests, this may not always be possible. However, the organisation offering the product may often be willing to develop customer-specific features for the product at its hourly invoicing price jointly agreed in the service agreement. From a commercial point of view, this is not significantly different in practice from custom software owned by the company. A custom product is originally made with a software partner for a fee, and if it is to be updated or modified during its lifecycle, the software partner is typically paid for the changes in accordance with the hourly invoicing price set in a framework agreement. Of course, the implementation of changes to custom software owned by the company can be put out to tender whereas changes to a product-based software may only be implemented by the product owner.

In the context of interchange servers, few product-based solutions are available in the market. This is due to there being hardly any demand for such solutions in the market (the market does not exist yet). As the C-Roads Platform specifications progress in relation to IP-based solutions for long-range communication, and national C-ITS services built in the Member States begin to be joined to each other, product-based solutions are also likely to emerge in the market to respond to this demand.

Currently, Monotch’s TLEX product, which also includes an interchange server segment, most closely resembles this type of product-based option. In Finland, the TLEX product has been utilised in the NordicWay3 experiment of the City of Tampere and Fintraffic Road Oy, and the use of the product has also been partially continued since then. At the same time, an integration pilot was carried out between the TLEX product and the Norwegian open source interchange server to test the functioning of the connection between them.

The development of the TLEX system began in the Netherlands in a situation where the C-Roads Platform specifications for long-range communication were not ready. As a result, TLEX is not fully compliant with the standards and, according to Monotch, they are waiting for the specifications to be completed before developing any new C-Roads Platform specifications. (Monotch interview 2024)

7.8 Discussion on the implementation of the interchange server

The implementation options of the interchange server were presented in the previous Section 7.7, which highlighted versatile ways of implementing interchange server. Below is a brief discussion of each implementation option from the perspective of the implementation of the Finnish interchange server.

Below is a list of some restrictions and assumptions related to this examination.

- It is not necessary to implement more than one interchange server in Finland, which will enable cross-border communication between C-ITS services across Europe in the future. One option (especially in the early phase) could involve joining the interchange server of another country from Finnish central C-ITS stations.
- In the future, the Finnish interchange server may also serve as an interconnection point for several central C-ITS stations that may emerge in Finland.
- Fintraffic Tie Oy is the most likely to serve as the interchange server operator (Kotilainen et al. 2023).
- The implementation of the interchange server may not be the most urgent part of the implementation of the C-ITS system (especially as long as the services are provided to end-users over mobile networks through mobile applications).

Table 12 presents the benefits and disadvantages of models for the procurement of interchange servers.

Table 12. Comparison of various implementation options for the interchange server.

Custom software implementation	
+ Flexibility of development + Independence + No potentially difficult product tendering process (possible mini-tendering process for expert resources within framework agreements)	- Price - Expensive lifecycle management - Requires the procurement of operational services for the service operating environment (server room/cloud service environment, management, monitoring and troubleshooting services as a separate procurement - Development needs are difficult to anticipate, and all require the work of external experts (changes caused by the environment, such as Commission requirements, end of support for the technologies used, adapting to continuous C-ITS growth)
Open source-based custom implementation	
+ Cost savings in the first implementation version thanks to the utilisation of open code + Flexibility of development	- Risks related to the used open source code (errors and security gaps that the open code may contain may be difficult to find, fixing situations involving errors requires a lot of work, will the actual developer provide assistance?) - Challenging to take over the open code (the creators have no experience of the previously created part, familiarisation with it takes time, generally acknowledged unwillingness among coders to utilise what others have done) - Expensive lifecycle management, potential benefits can be achieved through the development of open code - The above risks will particularly materialise if the open community is not made actively involved. - High operational service environment cost (server room/cloud environment, information security services, management, monitoring and troubleshooting services as a separate procurement)

	- Development needs that are difficult to anticipate
Open source community development	
+ Several funding providers participate in the development work + Eligible to EU grants + Flexibility of development (the community can decide on its direction, while a decision may be made to develop a specific product fork) + The development community provides support for its members in the implemented environment	- Administrative burden of establishing the community (governance models, defining a common goal, agreeing on funding, agreeing on joint practical operating models) - Differences in views regarding the direction of development during the process - High operational service environment cost (servers, clouds, telecommunications, security, management, monitoring, response and troubleshooting)
Product procurement	
+ Lower initial costs + Faster deployment + The product develops automatically with regard to new EU requirements related to the topic (usually included in the service price and may be required in competitive tendering) + The service price includes the operational service environment managed by the supplier (servers, clouds, telecommunications, security, management, monitoring, response and troubleshooting)	- Competitive tendering process - Challenges possibly posed by the change of contract periods regarding the change of product - Inflexible development (if the organisation has specific needs) - Vendor lock-in, particularly if the development of the solution results in a strongly customised implementation which is difficult to replace with products available in the market, and another risk caused by a large number of custom integrations with external systems; the risk is minimised if the solution is already standardised in terms of requirements and not subject to major customisation

In summary, an interchange server is a highly standardised solution based on the requirements set by C-Roads Platform. Its functionalities are similar wherever it is used as part of the European architecture of C-ITS services. Deployment of the interchange server does not require localization or custom integration with external systems. Based on this background, there may not be grounds for implementing a fully custom Finnish version from scratch.

Based on the information discussed above, product procurement or the utilisation of open source code emerge as strong options for the development of the interchange server. In both of these solutions, Finland should also carry out strategic planning related to the implementation method of this solution (and more broadly related to the development of the C-ITS sector).

In connection with product solutions, the product and service markets that may be created for Finnish companies should be taken into account as a part of the procurement of the product. When it comes to using open source code or engaging in community activities, it is important to develop a clear strategic plan. The planning aims to answer questions about how open source code is utilised, which licences are used, what is your role in the activities of the open community, how to ensure that you can influence the development and decision-making in the open community, how to ensure your competence while enabling business opportunities in the private sector.

Open community activities (e.g. at the Nordic level) could also offer significant opportunities for the Finnish (and Nordic) private sector. This would require the public administration to pay close attention to the private sector as a part of the open source development efforts. Strategic planning in partnership with the private sector could help clarify which components, such as essential core functionalities, are suitable for open community development, and which value-added layers could be left to the private sector. In this case, the public administration development work could bring considerable benefits to the private sector as a part of an open community. The private sector would also be able to participate in the open community activities (which would benefit the public sector) and, at the same time, could create significant business opportunities by producing its own added-value layers on top of the core components developed by the open community, use them as a basis of creating new commercial solutions and provide support services for them.

The methods described in the previous chapter should be a central part of the open source business strategy thinking and planning related to operating in an open source community. The measures aim to ensure that Finnish development work and investments simultaneously develop the Finnish transport system and the local business environment, which could even enable introducing Finnish innovations to the international market.

8 Privacy in C-ITS services

The protection of personal data and respect for privacy are fundamental European rights. The European Parliament has always stressed the need to maintain a balance between increasing security and safeguarding human rights, including data protection and privacy. (Fact Sheets on the European Union, 2025).

In C-ITS services, privacy protection and data protection are considered complementary concepts. The privacy protection focuses on the rights and freedom of choice of individuals in relation to their own data. It emphasises the protection of private life and the right to self-determination, and it also answers the question of "What data is collected and why?" Data protection, on the other hand, emphasises the legislative requirements for the technical protection and secure processing of collected data. It defines concrete measures for protecting data and stresses the secure processing and storage of data, in response to the question "How is data processed and protected?"

8.1 Privacy and data protection principles

The EU General Data Protection Regulation (EU 2016/679, GDPR) entered into force in May 2016 and has been applied since May 2018. It strengthens the rights of citizens and simplifies the rules applicable to businesses in the age of digitalisation. The GDPR aims to protect all EU citizens from privacy and information security violations in an increasingly data-intensive world, while creating a clearer and more coherent playing field for businesses. In Finland, the Tietosuojalaki (Data Protection Act, 1050/2018) specifies and supplements the GDPR and its national application.

The GDPR guarantees certain rights to data subjects. People have the right to be informed about how their personal data is processed, and they are entitled to access to the data that a company or organisation has stored about them. Every person has the right to the protection of their personal data. It is a fundamental right that safeguards the rights and freedoms of data subjects in the processing of their personal data. The purpose of data protection is to demonstrate when and under what conditions personal data may be processed while protecting the privacy of individuals and ensuring that their rights are respected.

Personal data is data that can be used to identify a person directly or indirectly, for example by combining individual pieces of data with other data that enables their identification. When assessing whether a piece of data constitutes personal data, the possibility of combining data becomes a key concept. This means that, for example, if a set of C-ITS message packets can be linked to a specific vehicle that can be linked to a specific vehicle identification number that can be linked to a specific registration number that can be linked to a specific vehicle tax recipient address, it becomes personal data that should be treated in accordance with legislation governing the processing of personal data. In other words, be aware that you may run into personal data in very unexpected contexts.

8.1.1 Principles of data protection

The principles of data protection must be observed whenever personal data is processed, and they must be followed throughout the life cycle of the processed personal data. The controller must also be able to demonstrate that the principles of data protection have been effectively implemented in the processing of personal data.

Processing of personal data

According to the data protection principles (individual principle in brackets), personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject (Lawfulness, fairness, and transparency)
- collected and processed for specific, explicit, and legitimate purposes (Purpose limitation)
- collected only to the amount necessary with regard to the purpose of the processing (Minimisation of data)
- updated when necessary – any inaccurate or incorrect personal data must be erased or rectified without delay (Accuracy of data)
- stored in a form which only permits the identification of data subjects for as long as is necessary for the purposes of processing the personal data (Storage limitation)
- processed confidentially and securely (Confidentiality and security).

To ensure that the processing of personal data to is lawful, there must be a legal basis, i.e. grounds, for it. This basis must be determined before the start of the processing. Once personal data processing is tied to a particular basis, that basis cannot be changed to another. Your choice of processing basis significantly affects what rights data subject have in relation to the controller. The controller must also be able to demonstrate their compliance with data protection legislation. The purpose of the obligation to demonstrate is to show how the data controller respects the privacy of data subjects, who are the subjects of personal data processing.

Grounds for processing personal data

The grounds for processing personal data include the following:

- The *consent* of the data subject, i.e. a voluntary declaration of intent by which the data subject approves the processing of their personal data.
- A *contract* when a person is a party to a contract – for example, when ordering goods online, the buyer can allow the seller to process their address information.
- A *legal obligation* based on EU or Member State law.
- The *protection of vital interests*, e.g. in situations concerning the life, death, or serious threat to the health of a data subject or another person.
- A task or public authority concerning the *public interest*, when so required by the public interest or the exercise of public authority vested in the controller. This can serve as a processing basis in both the private and public sectors in situations involving the public interest or the exercise of public authority in the EU or a Member State.
- Realising the *legitimate interest* of the controller when, for example, there is a meaningful relationship between the controller and the data subject –

for instance, when the data subject is a customer or subordinate of the controller. Legitimate interest requires the controller's own assessment using a balancing test. The public sector does not typically consider legitimate interests a suitable basis for processing, as other criteria – such as legal obligations or the public interest – are generally clearer and better suited to the public sector's statutory activities. (Office of the Data Protection Ombudsman, n.d., 'When is the processing of personal data permitted?')

8.1.2 Risk management

The controller must always assess the risks related to the processing of personal data before they begin processing any personal data. The purpose of a risk assessment is to help identify, assess, and manage the risks involved in the processing of personal data. It is intended as a continuous process for identifying and managing risks. One tool for risk assessment is the data protection impact assessment, which the controller can use when planning any activities that involve the processing of personal data. (Office of the Data Protection Ombudsman, n.d., 'Risk assessment and data protection planning')

The impact assessment describes the processing of personal data and assesses the necessity, proportionality and risks arising from the processing of personal data, as well as the necessary measures for addressing any risks. An impact assessment must be carried out whenever you intend to process personal data that is likely to pose a high risk to the rights and freedoms of individuals.

The objective of the impact assessment is to determine whether the remaining risk is justified and acceptable under the present circumstances. The impact assessment helps the controller to comply with, document, and demonstrate their compliance with the necessary data protection legislation. (Office of the Data Protection Ombudsman, n.d., 'Risk assessment and data protection planning')

Risk identification is especially important when the controller is defining the technical and organisational measures that they will use to ensure data protection in personal data processing. Technical and organisational measures refer to, for example, the instructions given to personnel for the implementation of data protection, access control implemented via self-monitoring, information system-related information security, data encryption, and other protective measures.

Risk assessment is a continuous activity. The adequacy of the measures must be continuously assessed in relation to the risk associated with the processing and updated whenever necessary. The controller is also responsible for demonstrating their compliance with their risk-based approach.

8.1.3 Transfers of personal data outside the European Economic Area

C-ITS messages are both generated in and sent to vehicles, so the role of the international automotive industry as the processor of the data must be taken into account with regard to privacy when data is processed outside the European Economic Area (EEA). A prerequisite for the transfer of personal data outside the EEA is that the processing of personal data must be permitted in the situation in question and that the transfer of personal data must be based on a transfer basis specified in Chapter V of the EU General Data Protection Regulation (GDPR). The effectiveness of the transfer basis and the need for additional safeguards must be assessed on a case-by-case basis.

The primary transfer basis is a decision issued by the European Commission on the adequacy of data protections (so-called 'adequacy decision'): if the European Commission has decided that a specific third country, territory, sector, or international organisation has ensured an adequate level of data protection, personal data may be transferred directly based on this adequacy decision.

If no adequacy decision exists, the controller must determine whether personal data may be transferred on other grounds, such as standard clauses or based on binding corporate rules. If it is not possible to transfer personal data based on an adequacy decision or other transfer bases, the controller can still determine whether personal data can be transferred on the basis of a derogation for specific situations. (Office of the Data Protection Ombudsman, n.d., 'Transfers of personal data out of the European Economic Area')

8.1.4 Transfer Impact Assessments

A Transfer Impact Assessment (TIA) is required when personal data is transferred outside the European Union (EU) or the European Economic Area (EEA) and no adequacy decision has been made. A TIA can be used to assess the legality of a transfer and ensure that the recipient country has an adequate level of data protection in place that corresponds to, for example, the requirements of the General Data Protection Regulation (GDPR).

The GDPR does not explicitly require a TIA as a separate concept, but the EU's data protection authorities and the European Data Protection Board (EDPB) have highlighted its importance as part of the fulfilment of Chapter V of the GDPR. Especially in situations where personal data is transferred outside the EU or EEA without an adequacy decision, the TIA is considered a vital part of the introduction of appropriate safeguards and risk management. (Office of the Data Protection Ombudsman, n.d., 'Safeguards to supplement transfer tools')

8.1.5 Informing data subjects

In particular, data subjects must be informed of the purposes for processing their personal data and the legal basis for the processing. If the personal data has not been obtained from the data subject, you must also report the categories of personal data in question. In addition, the data subject must be transparently informed of the recipients or groups of recipients of the personal data, international data transfers, the storage period of the personal data, the rights of the data subject and automated decision-making, and any further processing before the processing in question. (EU 2016/679, 2016)

The term 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The controller is obliged to assess the risk level of the event, document it accordingly, and notify the supervisory authority. The data subject must be notified of a personal data breach if it is likely to pose a high risk to their rights and freedoms. No notification is necessary if the appropriate technical and organisational safeguards have been implemented and applied to the personal data affected by the personal data breach, or if the controller has taken further measures to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise. (Office of the Data Protection Ombudsman, n.d., 'Personal data breaches')

8.1.6 Rights of the data subject

The data subject has the right to obtain information on the personal data to be processed and its origin, the purposes and legal basis for the processing, the categories of personal data to be processed (if the data has not been obtained from the data subject), the recipients or groups of recipients to whom the data subject’s personal data has been disclosed, and the period of storage of the personal data or the grounds for determining it. In addition, the data subject has the right to request the rectification, erasure, or restriction of the processing of their personal data and to object to its processing and not be subject to automated decision-making. The data subject’s data must be transferable to another controller, unless prevented by any technical limitations.

The data subject cannot exercise all of their rights in all situations – these rights may be limited by, for example, the basis on which the personal data is processed. (Office of the Data Protection Ombudsman, n.d., 'Rights of the data subject')

8.1.7 Anonymisation and pseudonymisation of personal data

Personal data is such data that can be used to identify a person directly or indirectly, for example by combining individual pieces of data with other data that enables their identification. A person can be identified by, for example, their name, address, personal identity code, vehicle registration number, IP address, or other distinguishing characteristic.

The EU General Data Protection Regulation (EU 2016/679, GDPR) protects personal data regardless of the technology used in its processing. The way in which the data is stored is also considered immaterial – it can be stored in, for example, an IT system, video monitoring system, or paper archive. As long as the data can be used to identify a person directly or indirectly or it can be reconverted into an identifiable form, it will remain personal data and be subject to the GDPR.

The technical solutions for privacy protection can be divided into (i) anonymisation and (ii) pseudonymisation. Anonymisation refers to the permanent deletion of identification data and the aggregation of data without any unique identifiers. The prevention of identification must be permanent and make it impossible for the controller or a third party to reconvert the data into an identifiable form with the information held by them. The anonymisation process must take into account all reasonably viable methods for reconverting the data into an identifiable form. The controller must also prepare for the possibility that the anonymisation may be weakened over time and due to technological advancements. Whether an individual data item can be considered anonymous or not requires case-by-case evaluation. Individuals can be identified through other data points than just their names. In other words, the deletion of names and other identification data is not always sufficient for rendering the data in a personal data file fully anonymous. Anonymised data is no longer considered personal data and is not subject to any data protection provisions. (Office of the Data Protection Ombudsman, n.d., Pseudonymised and anonymised data)

Pseudonymisation refers to the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information. For example, the encoding of personal data is a form of pseudonymisation. Encoded data cannot be linked to a specific person without a code key. However, the holder of the code key can decrypt the dataset and re-identify each data subject.

In the C-ITS environment, pseudonymisation means changing identification data and the prevention of links between different services. The EU's C-ITS Security Credential Management System (EU CCMS) is based on this approach. An example of this is the protection of the communication privacy of mobile C-ITS stations (vehicles). The sender of the message uses variable authorisation tickets (ATs) for their communications. The AT is used to confirm the right of the communicator to participate in the communications of certain C-ITS services (message types). They function as short-term certificates, enabling communications without revealing the actual identity of the device or vehicle. As the data is pseudonymised, it can be used to identify individual users in a group and combine them with different datasets. Pseudonymised data is still personal data, i.e. its processing is subject to data protection provisions.

The EU C-ITS security management system uses PKI (Public Key Infrastructure) authentication to ensure the reliability and security of its messages. Technically, the PKI infrastructure can be complemented with advanced cryptographic methods, such as Zero-Knowledge Proofs, Group Signatures, and Blind Signatures. The PKI method allows the Certificate Authority to uniquely identify the vehicle or link it to other data, such as a camera image. In this case, Group Signatures, for example, can be used to extend the security of a group while also allowing its members to remain anonymous while they communicate. This promotes the reliability of messages while preventing the direct identification of individual vehicles (Yue et al. 2022). However, C-Roads Platform profile specifications and ETSI specifications continue to focus on more traditional methods and have not yet defined such additional security measures.

8.2 Privacy requirements for C-ITS messages

The EU's proposed Delegated Regulation on C-ITS (C/2019/1789) was not adopted during the EU Parliament's deliberations in 2019, which means that the protection and processing of personal data in the context of C-ITS services is currently strongly linked to general regulation at both the national and EU level. Annex 4 to this proposed regulation focused specifically on C-ITS security policy, but there is no information yet on the reopening and processing of the proposed regulation. However, the rejected proposed regulation and the evaluations based on it have served as an important starting point for the definition and development of C-ITS services, including its privacy-related measures.

8.2.1 EU-level requirements

The key regulatory mechanisms at the EU level are:

EU General Data Protection Regulation (EU 2016/679, GDPR): The processing of personal data in EU Member States is regulated under the GDPR. C-ITS privacy has been built and evaluated in relation to the GDPR's principles.

The **revised ITS Directive (EU/2023/2661)** underlines data protection and privacy rules in accordance with the GDPR. The personal data defined in the ITS Directive may be processed for the purpose of ensuring the safety and security of road traffic and enhancing the management of traffic, mobility, or disruptions. The Directive requires that any impact assessments include an analysis of the impact on the protection afforded to individuals with regard to the processing of their personal data. Anonymisation must be used whenever technically possible. If anonymisation is not technically possible, the data must be pseudonymised where possible.

ePrivacy Directive (2002/58/EC): Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector applies to the processing of personal data that is related to the provision of publicly available electronic communications services over public communications networks. It requires ensuring the confidentiality of communications and the related communications data.

The purpose of the Directive is to supplement general data protection regulations and protect the fundamental rights of natural persons, in particular their right to privacy, and the legitimate interests of legal persons. The Directive permits the processing of spatial data required for the transmission of communications on mobile networks, when said data is considered necessary telecommunication data. The telecommunication data must be deleted or made anonymous when it is no longer needed for the transmission of communications. Spatial data other than telecommunication data may only be processed if it has been made anonymous or if the users or subscribers have given their consent to its use. The data may only be processed to the extent and for the period that is necessary for the provision of the added value services. The possibility of the mobile network to process more detailed spatial data and provide added value services for the purposes of personalised traffic-related notices or guidance is only permitted with the client’s consent.

The Directive also provides for the storage of data or the use of data stored on the subscriber’s or user’s terminal device. Telecommunications companies must take the appropriate technical and organisational measures to ensure the security of the services they provide.

European Data Prtection Board (EDPB): The role of the EDPB is to provide guidance on the interpretation of the core concepts of the EU General Data Protection Regulation (GDPR) and make binding decisions in disputes concerning cross-border processing operations, to ensure the uniform application of EU regulations and avoid differing rulings on the same cases in different jurisdictions. The EDPB has issued an opinion in the context of connected vehicles and mobility applications, but C-ITS is excluded from this guideline (European Data Protection Board 2021, 11).

Cybersecurity regulations: The assessment and certification of C-ITS device security requires the approval of a national or international certification authority.

The **European AI Act (EAA)** classifies the risk levels of AI systems and sets requirements for them. The EAA complements other data protection and information security frameworks (such as the GDPR) by providing AI-specific safeguards for C-ITS services and connected vehicles.

Data Governance Act (EU 2022/868): The Act focuses on data management and promotes the creation of secure data sharing mechanisms, enabling cooperation between the public and private sectors. It aims to increase trust in the use of data by setting rules that protect the privacy and security of data. This can help facilitate the deployment of C-ITS services.

Data Act (EU 2023/2854): The Act aims to regulate who can access and use data in the EU. It aims to promote competition and innovation by clarifying data access rights and safeguarding equity in data value chains. The Act also allows for registered data forwarding services.

8.2.2 National requirements

National data protection supervision: In Finland, compliance with data protection legislation is supervised by the Data Protection Ombudsman. The Finnish Transport and Communications Agency Traficom is responsible for supervising compliance with the Act on Electronic Communications Services and the regulations and decisions issued under it. However, the Data Protection Ombudsman supervises compliance with the provisions presented in Chapter 20 of the Act on the processing of location data.

Data Protection Act (1050/2018)

The Act specifies and supplements the General Data Protection Regulation (GDPR) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data, as well as its national application. For example, the Act specifies the powers and procedures of the Finnish Data Protection Ombudsman in more detail.

The supervising authority (Office of the Data Protection Ombudsman) has investigative powers and the right of access to information. Data subjects have the right to refer a matter to the Data Protection Ombudsman for consideration if they believe that the relevant legislation is being infringed in the processing of their personal data. The supervisory authority may impose a conditional fine to support the aforementioned orders, restrictions on the processing of personal data, or interruptions of data transfers. (Data Protection Act 1050/2018)

In the context of C-ITS, the Data Protection Act supplements the appropriate and special measures for the processing of personal data and introduces more detailed technical, procedural, and organisational measures to protect the rights of data subjects.

Act on Electronic Communications Services (917/2014)

The national implementation of Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) has been realised primarily through the provisions in Chapter 17 of the Act on Electronic Communications Services (917/2014).

With regard to national legislation, the Act on Electronic Communications Services deals with the confidentiality of communications and the protection of privacy. Chapter 17 specifies the processing of electronic communications and traffic data. traffic data means information that can be associated with a legal or natural person and is processed for the purpose of the conveyance of a communication as well as information on the call sign of a radio station and the user of the radio transmitter, and on the starting time, duration or transmission site of a radio transmission.

Radio communications intended for public reception and its traffic data may be processed in accordance with Section 136 in the case of, for example, distress signals and radio communications intended for public reception. Other electronic communications and traffic data may be processed with the consent of the party to the communication or if so provided by law. Whoever receives or obtains in any other way knowledge of electronic communications, radio communications, or traffic data not intended for them must not disclose or make use of the content or traffic data of such communications, or the knowledge of its existence, without the consent of a party to the communication, unless otherwise provided by law. (Act on Electronic Communications Services 917/2014)

The processing of electronic communications and traffic data is only permitted to the extent required by the purpose of the processing and must not restrict the protection of confidential messages and privacy beyond what is necessary. The purposes of the processing can include the conveyance of communications, the technical development of communications services, statistical analysis, or the detection, prevention and investigation of misuse. (Act on Electronic Communications Services 917/2014, Sections 141–143).

Electronic communications and traffic data may only be disclosed to those parties entitled to process them in the given situation. After processing, electronic communications and traffic data must be destroyed or rendered such that they cannot be associated with the subscriber or user involved, unless otherwise provided by law. Electronic communications and traffic data may only be processed by a person acting on behalf of a communications provider or a subscriber. (Act on Electronic Communications Services 917/2014, Section 137).

Messages and traffic data may only be processed to the extent necessary for the conveyance of communications, performance of the agreed service, and for the purpose of ensuring information security as provided in Section 272. (Act on Electronic Communications Services 917/2014, Section 138).

A communications provider shall record a detailed event information on processing of traffic data in data systems containing traffic data essential to confidentiality and protection of privacy, if this is technically feasible without unreasonable cost. This event information must show the time and duration of the processing and the person performing the processing. The event information shall be stored for two years from the date on which it was recorded. (Act on Electronic Communications Services 917/2014, Section 145).

The Act on Electronic Communications Services can be applied to C-ITS services, as they represent the ‘added value services’ referred to in the Act (location and presence service). Provisions on location data and the processing of other subscriber connection or terminal device location data are laid down in Chapter 20 of the Act. In the context of C-ITS, this has a particular impact on the privacy of messages that make use of long-range communication. The Act lays down provisions on the processing of communications and traffic data, which also cover IP-based messages implemented in mobile networks. Communication intermediaries, such as telecommunications companies, are obliged to process traffic data legally while ensuring the protection of privacy. The processing of traffic data must be justified in terms of the provision of the service, and their storage is limited to certain statutory purposes. A telecommunications company may process traffic data for needs related to the provision of a service, but sharing this data to third parties is generally prohibited without the consent of the party to the communication or other grounds laid down by law. Telecommunications companies are obliged to protect the data they collect and retain it only for a certain period and only for essential reasons.

C-ITS services may store and use vehicle data and the data from users' terminal devices. Provisions on the storage of data describing the use of the service on the user's terminal device and the use of this data are laid down in Section 205 of the Act, which implements Article 5(3) of the ePrivacy Directive. According to it, the storage of cookies or other information describing the use of the service on the user's terminal device and the use of this information is permitted for the service provider if the user has given their consent and the service provider provides the user with clear and comprehensive information on the purpose of the storage or use. This does not apply to the storage or use of data where the sole purpose is to carry out the transmission of a message on a communications network or which is necessary to the service provider for the provision of a service specifically requested by the subscriber or the user of the service. The storage and use is only permitted to the extent required by the service and must not restrict the protection of privacy beyond what is necessary.

The **Act on the Protection of Privacy in Working Life (759/2004)** regulates matters concerning the privacy of employees in working life. Employers have an obligation to collect and store personal data on their employees. Employees and applicants, on the other hand, must provide this data to the employer. With regard to C-ITS, V2I messages, for example, are likely to contain personal data, so employers must comply with the necessary GDPR obligations when processing this data.

8.2.3 C-ITS-specific requirements for privacy

The proposed C-ITS Regulation (C/2019/1789) describes the EU CCMS, while Annex IV in the Regulation describes the C-ITS security policy, which defines the information security management requirements for C-ITS. As described in Chapter 3.1, despite the rejection of the Regulation, the European Commission began promoting the deployment of C-ITS services in ways consistent with the principles of the C-ITS security and certificate policy. The work for defining privacy protection has continued together with data protection development experts from various organisations: the EU Joint Research Centre (JRC), the C-Roads Platform cooperation group, and the standardisation organisation ETSI.

EU Joint Research Centre (JRC) Security Policy

The policy document prepared by the JRC (C-ITS Security Policy, 2023, *4–5*) is an updated version of Annex IV to the proposed C-ITS Regulation. It defines the C-

ITS security policy in Europe and is closely linked to the EU's C-ITS Certificate Policy (2024). The aim of the C-ITS Security Policy is to provide a framework for information security management in the deployment and operation of the European C-ITS. It defines how information security is managed, including the definition of information security policies for individual stakeholders and the functions of the information security management system. The C-ITS Security Policy requires that C-ITS stations are operated in accordance with the requirements of ISO 27001 or NIS 2 and that all C-ITS station operators comply with the document's requirements.

The document presents a classification framework for the management of information security and data protection in the deployment and operation of C-ITS. Its key approach is to ensure the *confidentiality, integrity, and availability* of information. The document emphasises the classification of data according to the identified risk: low, moderate, and high, where the potential impacts on the organisation's operations and the priorities of information security measures are assessed accordingly. These are described in more detail in Chapter 4.2.3.

The protection of personal data falls under the classification of 'confidentiality'. The impact of any unauthorised use of data should be assessed on a scale of (i) limited, (ii) serious, (iii) severe or catastrophic. In addition, the document sets minimum impact values for processed data that must be followed by C-ITS stakeholders in both fixed and mobile C-ITS stations. While this classification helps to prioritise security measures, all messages must be adequately protected to avoid any harmful consequences. (Table 13)

Table 13. Minimum impact values for C-ITS messages for the prioritisation of security measures (C-ITS Security Policy, 2023).

	Message profile information from fixed C-ITS stations	**Message profile information from mobile C-ITS stations**
Confidentiality	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: low	CAM: low DENM: low SREM: low Personal data contained in these message profiles: moderate
Integrity	CAM: moderate DENM: moderate IVIM: moderate MAPEM: moderate SPATEM: moderate SSEM: moderate	CAM: moderate DENM: moderate SREM: moderate
Availability	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: moderate	CAM: low DENM: low SREM: moderate

C-Roads Platform

The cooperation group for the C-Roads Platform (C-ITS Security & Governance, 2023) has also defined requirements for the privacy of C-ITS messages. The key object of the specification is the EU CCMS and the protection provided by the previously described C-ITS Certificate Policy (2024) and various communication technologies, such as the ETSI security envelope and IP-based communications. These also play an important role in the protection of personal data. With regard to privacy, the C-Roads Platform documentation contains some more detailed requirements:

Anonymity: Vehicles and station sending C-ITS messages use pseudonyms, i.e. they send messages using identifiers that do not directly reveal the user's identity. These identifiers should be changed regularly to reduce the possibility of monitoring an individual object for long periods of time.

Technical and organisational separation: The C-ITS certificate policy determines the technical and organisational separation of certain roles as a general planning principle. The roles of the Enrolment Authority (EA) and the Authorization Authority (AA) are completely separate. They include the separation of processes related to long-term keys (signing a certificate application) and short-term keys (authenticating individual messages).

The use of certificates: Short-term certificates that are used to sign messages are regularly changed in C-ITS stations during operations, and the reuse of certificates is restricted. This helps reduce the possibility of tracking or monitoring a particular user over the long term. The C-ITS certificate policy specifies that up to 100 certificates can be active at a time during a one-week validity period.

Data protection and data retention periods: Any personal data contained in messages, such as certificates and identifiers, should not be stored for longer than five minutes to maximise privacy. This short time limit, which applies to V2I messages in particular, aims to prevent the long-term accumulation and use of personal data for unspecified purposes.

Authentication and elevation: All stations that send messages must have the appropriate certificates for verifying the authenticity of messages. These certificates are short-term and expire quickly, which means that their continuous rotation is important for ensuring information security.

Communication security: Different communication technologies, such as broadcast- and IP-based messages, must be secured in accordance with the ETSI TS 103 097 standard. This includes the use of digital signatures to ensure the integrity and reliability of messages.

The **C-Roads** Platform **Security and Governance document** highlights the fact that privacy issues differ between different station types. Vehicle C-ITS stations that provide C-ITS services to (private) end-users need varying (pseudonymous) signatures in accordance with the given requirements. This privacy requirement does not necessarily apply to roadside stations, road operator vehicles, or central C-ITS stations that sign and send messages on their behalf. In addition, the document notes that data protection does not apply to communications from roadside stations to road users (I2V), as these **I2V services do not process personal data**. It should be noted that the vehicles of road operators and road transport authorities that include C-ITS stations may be subject to special regulation. This regulation applies in particular to the supervision of employees and the right to privacy of the persons using the vehicles. (C-ITS Security & Governance, 2023)

ETSI standards

With regard to data protection, the C-Roads Platform profile specifications require interoperability with ETSI standards (ETSI TS 102 941 V2.2.1, 2022 and ETSI TS 103 097 V2.1.1, 2022).

The **ETSI TS 102 941** document defines the requirements for trust and privacy management in Intelligent Transport Systems (ITS). The most important privacy requirements include the prevention of PKI pseudonymity and links between different identifiers. Linking can be prevented by minimising the amount of data that does not change or changes very slowly over time. If detailed and unchanged data, such as a vehicle's serial number or other very permanent information (such as certain device settings), are included in several messages, it may allow these messages to be linked to the same vehicle over a longer period of time. Linking prevention can be implemented by using temporary and frequently varying identifiers, as these prevent any attempts at connecting the transmissions made by the same vehicle over time – for example, by making it impossible for two identical transmissions to occur on different dates.

The document also emphasises the lifecycle management of C-ITS stations, starting at the manufacture of the station and including its registration and authorisation, and finishing at the end of its lifecycle. During this period, safety and privacy are ensured through various technical and organisational measures throughout its lifecycle.

ETSI TS 103 097 defines the ETSI security envelope used for C-ITS messages, the content and presentation of certificates included in the security envelope, and the protection profiles for CAMs and DENMs. The standard focuses on the formats of security headers and certificates but does not specifically address linking prevention or other aspects related to privacy.

8.2.4 Accountability and management system ISO/IEC 27701

Accountability is a key principle of the EU General Data Protection Regulation (GDPR). The purpose of demonstrating one's compliance is to show how the controller respects the data protection of their data subjects, i.e. those subject to the processing of personal data.

This accountability can be verified via the data privacy extension ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002, as the implementation of the controls outlined in Annex A (Controller) will confirm the organisation's compliance with GDPR obligations. Annex B describes the obligations of the processor. Compliance with ISO/IEC 27701 facilitates the assessment of accountability, improves quality, and clarifies the obligations under data protection legislation.

The data privacy extension provides clarifications on the requirements and controls presented in ISO/IEC 27001 and ISO/IEC 27002. For data protection, the extension presents additional requirements for the organisation's operating environment and planning, while in the case of controls, the extension includes instructions and additional information concerning the implementation of the controls. Regarding data protection, the instructions and information specify all other controls except those related to business continuity.

Requirements

In the organisational environment, the organisation defines its role concerning personal data processing. The requirements help identify data protection legislation, regulatory requirements, and contractual obligations that the organisation must comply with. Compliance can be verified through a personal data management system.

Planning is used to define the data protection assessment and processing procedure that identifies the risks associated with the processing of personal data and ensures that they are appropriately managed. The information security policy must be expanded to include data protection, and the objectives defined in it must take data protection into account.

Data protection controls

The information security policy must support the organisation’s role in accordance with its operating environment, as well as its compliance with the requirements of its internal and external stakeholders. The organisation must designate a role (data protection officer) to be contacted in matters concerning the processing of personal data and assign resources to ensure the implementation of its compliance management. The information security incident management process must take the identification of personal data breaches into account. The process describes the necessary reporting obligations: official notifications, stakeholder notifications, notifications to the data subject, and the obligation to record personal data security breaches.

The awareness of the organisation's personnel regarding the impacts of personal data processing, including incident reporting, must be maintained. Increasing their awareness must cover the identification of personal data breaches. The proper processing and classification of personal data must be ensured, and this includes the organisation’s subcontracting chain. Compliance with personal data processing rules must be ensured throughout the entire lifecycle of personal data processing. Additionally, the rules for personal data processing must cover the processing of log data. Compliance is ensured through confidentiality agreements. Personal data must be protected with encryption during data transfers.

Asset management and the personal data contained within, especially sensitive personal data, must be protected with encryption. The devices used for processing personal data must be secured with appropriate protection throughout their lifecycle, with particular attention given to secure physical disposal.

User accounts that are disabled or outdated in systems and services processing personal data should not be restored to users once their access rights lifecycle has ended. The organisation must use log management to identify the actions of users authorised to process personal data. Authentication must be implemented through secure authentication measures.

The backup policy must consider the statutory and contractual requirements and restrictions related to the processing and deletion of personal data. The integrity of the data in backups containing personal data must be ensured during the recovery process. Logs of restoration activities must be maintained. If backups are stored by a subcontractor, they must only be handled by authorised parties and protected using encryption. The implementation of these protective measures is ensured through subcontracting agreements.

The log data must include detailed information on the use of personal data, such as additions, modifications, and deletions. The processing of log data covers the subcontractor's processing of personal data. The log data must only be available to authorised processors and separated by each customer if necessary. When managing log data, it should be noted that personal data may not be stored for longer than is necessary for the processing.

During the lifecycle of secure development, the requirements for the protection and minimal processing of personal data must be considered. The risks of the processing of personal data are assessed with a data protection impact assessment, which serves as the basis for defining the necessary protection needs in the context of secure development. The basic goal of the lifecycle of secure development is data protection by design and by default, including in the subcontracting chain. Authentic personal data should not be used in the processing of test data. If this cannot be avoided, the appropriate protection of personal data must be considered. Personal data must be appropriately destroyed when processing is no longer necessary.

When an organisation acts as a personal data processor, it must provide clients with independently produced evidence that the implementation of information security supports data protection. Additionally, technical evidence of the execution of permitted processing can be produced, including the results of vulnerability testing.

Risk management requires accountability

When an organisation carries out a data protection impact assessment under the EU General Data Protection Regulation (GDPR), the organisation fulfils its accountability obligation for risk management. The privacy extension ISO/IEC 27701 provides concrete tools for accountability and is therefore an important document for the controller of C-ITS personal data.

8.2.5 *Assessments of the implementation of privacy protection in C-ITS messages*

The proposed C-ITS Regulation (C/2019/1789) was rejected, but the specification and assessment made for it form a crucial foundation for evaluating C-ITS messages and privacy protection. This chapter focuses on a few key assessments.

Article 29 Data Protection Working Party

The Article 29 Working Party (WP29) was an independent European advisory body that extensively addressed issues related to data protection and personal data. WP29 had a significant impact on the way data protection issues are dealt with in Europe and its legacy continues through the EU General Data Protection Regulation (GDPR) and the European Data Protection Board (EDPB).

In its statement titled "*Processing personal data in the context of C-ITS*" (Article 29 Data Protection Working Party, 2017), WP29 discusses the processing of personal data in the context of C-ITS messages. The statement covers only short-range data transmission solutions but is otherwise a comprehensive document regarding the C-ITS security credential management system (EU CCMS).

The statement clearly outlines that C-ITS data is personal data and emphasizes the minimization of collected data. To enhance data protection, WP29 lists several recommendations that are still valid today:

- The Commission should draft a roadmap for lawful processing of location data of EU citizens in the context of C-ITS applications, where the enactment of an EU-wide legal instrument is the ultimate goal (art 6(1)c of the GDPR).
- Regarding the grounds for processing, the Commission should begin drafting an EU-wide legal instrument as soon as possible. Such a legal obligation should not allow the general collection and processing of personal data, but the scope of the legal obligation should be properly assessed.
- Other grounds for processing (consent, performance of a contract, legitimate interest, public interest) can only be used if the critical issues identified in the document for each of them can be solved. For public interest, an assessment is required on how the collected data impacts data subjects and their privacy expectations, and further safeguards are needed from a technical perspective.
- The data protection impact assessment (GDPR Article 35(10)) should be prescribed during the legislative process to clarify any risks and mitigation measures from the outset.
- In all chosen legal bases, pre-installed C-ITS functions must be disabled by default.
- The provisions of Article 25 (Protection by design) of the GDPR must be implemented to allow users to select their preferred monitoring options (time, frequency, locations).
- Security should be enhanced to prevent use of C-ITS data beyond legitimate purposes.
- Other privacy design solutions, such as data generalization or noise, should be implemented to limit unnecessary exposure to long-term tracking.
- Special attention should be paid to the frequency of certificate changes to balance between the chosen rotation interval and the risks of long-term tracking.
- Information relating to criminal convictions and offences should not be sent.
- Data quality should be carefully assessed to reduce the risk of false alarms or misinterpretations of actual emergencies.
- All parties involved in the C-ITS platform should clearly indicate how long they retain data, and all C-ITS operators should be prohibited from creating a centralised database of exchanged messages.

Following the statement, progress has been made. For example, the C-Roads Platform has led the efforts to develop the certificate exchange and further clarify their specification. The qualitative assessment of collected data has been advanced in various forums, but ultimately the signatory of the C-ITS message is responsible for the reliability of the data. In the absence of a Delegated Regulation on C-ITS requirements, legislative-demanding issues remain open.

European Data Protection Board (EDPB)

The European Data Protection Board (EDPB) is an independent European body and an umbrella organisation that brings together the national data protection authorities of the countries in the European Economic Area and the European Data Protection Supervisor.

The EDPB has issued its opinion on the processing of personal data related to connected vehicles and mobility applications (European Data Protection Board, 2021). According to the EDPB, C-ITS data protection issues are very specific (due to e.g. unprecedented amounts of location data, the continuous transmission of personal data, the data exchange between vehicles and other road infrastructures) and their processing continues at European level. Therefore, C-ITS personal data has been excluded from the EDPB's statement. Regarding C-ITS, the EDPB refers to the stance of its predecessor, the Article 29 Data Protection Working Party. However, the EDPB's statement provides a slighty more recent insight into its attitude towards use cases and data similar to those in C-ITS. Additionally, the handling of data protection concerning the emergency call system in vehicles, eCall, can be regarded as a kind of precedent

The EDPB emphasises that the use of spatial data requires special protective measures to prevent the monitoring of individuals and the misuse of data. The information can reveal not only the driver’s workplace and place of residence, but also their leisure time interests and possibly sensitive details, such as their religion or sexual orientation, based on the locations they visit.

Additionally, the document emphasises that the drivers and passengers of vehicles may not be sufficiently informed about the data processing done in or through their vehicles. Information may only be provided to the owner of the vehicle, who may not be the driver. The ownership of a vehicle can also change, due to it being sold or rented. The EDPB stresses that if the data processing is based on consent, all elements of valid consent must be fulfilled. This means that consent must be free, specific and given based on an informed choice, and it must represent the clear will of the data subject.

Data controllers must pay special attention to the procedures for obtaining valid consent from different participants, such as vehicle owners or users. According to the ePrivacy Directive, consent must be obtained from the user or the subscriber. The consent must be given separately for specific purposes and should not be linked to a contract related to the purchase or renting of a new vehicle. The data subject must be able to withdraw his/her consent as easily as they gave it. In the context of C-ITS messages, this poses significant challenges in using consent as a basis for processing.

The consent requirement applies under Article 5(3) of the ePrivacy Directive (as well as per the GDPR) when storing information or accessing information already stored in connected vehicles. This requirement can be removed in two specific situations. If storing information or accessing it is necessary solely for transmitting communications in an electronic communications network, consent is not required. Consent is also not required when storing information or accessing it is necessary to provide an information society service expressly requested by the user or subscriber. This means that if a user, for example, requests GPS navigation services that require access to the device's internal information, consent is not mandatory.

Law enforcement authorities may require the processing of data collected by connected vehicles. In this case, such data will be considered to relate to criminal convictions and offences under the conditions set forth in Article 10 of the GDPR and other applicable national legislation. The EDPB notes that the processing of personal data solely to comply with requests from law enforcement authorities does not constitute a specific, explicit, and legitimate purpose under Article 5(b) of the GDPR.

However, when the ePrivacy Directive does not require the consent of the data subject, the controller is responsible for choosing the legal basis under Article 6 of the GDPR that is best suits the processing of the personal data (European Data Protection Board, 2021, 14).

National Road Authorities’ TIARA project

The TIARA (Trusted Integrity and Authenticity for Road Applications) project provides each National Road Authority (NRA) with a broader view and information on what is required to achieve a reliable and secure information infrastructure. The purpose of the draft report (Maerivoet & Ons 2023) is to ensure that road users can trust road operators to process C-ITS data by lawful and appropriate means. The report helps road operators understand the impacts of processing road user’s location data on privacy protection and offers recommendations for handling this data.

The document identifies several types of personal data collected from the data subjects, such as location data, biometric data, technical vehicle data, driving behaviour data, and information contained in infotainments systems.

The starting point of the report is that C-ITS messages constitute personal data. They are considered as such mainly due to the use of PKI certificates, along with message header field information, timestamps, and possible measurements of the vehicle in question. The authors highlight experiences from the ViaPass project conducted in Belgium, where data has been systematically collected from vehicle units using pseudonymization for heavy vehicles. The project has demonstrated how vehicle tracking can still be executed despite having only a minimal number of location points (Maerivoet & Ons 2023, 18). The report has reviewed privacy research reports outside the C-ITS context, so direct conclusions should be avoided.

The report emphasises that the data protection of vehicles used in Europe is primarily governed by the EU General Data Protection Regulation (GDPR). In accordance with the GDPR and the EDPB's guidelines, data subjects are granted the right to access, correct, and delete data concerning them. This ensures that users have a significant amount of control over the processing of their personal data. Built-in data protection plays a key role in the creation of ecosystems for connected vehicles. The guidelines emphasise the importance of minimising the data to be collected and processed, as well as the need to communicate openly to data subjects about the processing of the data. Many car manufacturers consider strict regulation beneficial because it is believed to ensure consumer trust, which is essential for the large-scale utilization of C-ITS (Maerivoet & Ons 2023, 43–46).

The report assesses the possibilities related to identifying an individual vehicle and breaking the anonymisation of location data, i.e. deanonymisation. To mitigate these risks, the report provides an overview of the measures and methods used to mitigate risks and assesses the need for further measures. The additional risk management measures represent technological, regulatory, and organisational approaches to securing data protection and privacy in the processing of vehicle data. The methods include a combination of anonymization, new cryptographic methods, and minimizing data quantity, suspending data exchange in critical areas such as homes and workplaces, and utilizing blockchain technology. The C-Roads Platform specifications do not yet include these methods.

The primary purpose of impact assessments is to determine what information C-ITS messages can reveal about road users and the potential impact of data disclosure on individuals. The benefits of C-ITS data, including improved traffic safety, are significant, but they also involve considerable privacy risks. Closer attention must be paid to the correlation of vehicle data – such as location, speed, and directional data – with personal data. These are discussed in more detail in Chapter 8.5.1. The increase in advanced analysis techniques has also increased the likelihood of identifying individuals from pseudonymised data, making the continuous development of current and future data protection measures a clear necessity. An impact assessment is necessary to understand how different data combinations and analyses can affect individuals’ privacy.

Overall, the document recognizes the importance of data subject rights in GDPR-compliant personal data processing, and it requires that data processors adhere to these rules and safeguards to protect data and fulfil data subject rights. The existing regulation's role is seen as defining more the outcome and principles. Member States and industry stakeholders must independently determine the best technical measures to meet these requirements. (Maerivoet & Ons 2023, 59).

8.2.6 eCall as precedent

eCall, the emergency call system for vehicles, has been mandatory for new vehicle models in vehicle categories M1 and N1 (passenger cars and vans) since 2018. The eCall in-vehicle system unit sends a minimum set of data (MSD) to the emergency response centre and opens a voice connection between the vehicle and the emergency response centre. The eCall MSD includes information on the location and date of the accident, as well as the VIN, vehicle category, and driving power of the vehicle.

In its statement, the European Data Protection Supervisor (EDPS) highlighted the implementation of privacy protection in the eCall system as an example (European Data Protection Board, 2021, 30). In the absence of a statement on a C-ITS implementation, it could potentially be interpreted as a good precedent.

The general framework for the regulation of personal data-related processing is the GDPR. Additionally, the ePrivacy Directive (EU 2002/58, 2002) sets regulations for entities wishing to store or access data stored on a subscriber's or user's terminal equipment in the European Economic Area (EEA). An essential starting point is that the regulation on the eCall system (EU) 2015/758 overrides the need for driver consent for the processing of location data and personal data transmitted in the eCall minimum set of data (MSD) and constitutes a legal obligation for data processing under the GDPR. (European Data Protection Board 2021, 31).

The regulation governing the operation of the eCall system (EU) 2015/758 states that data processed under this regulation should not be retained longer than required for emergency handling. Data stored in the internal memory of the eCall vehicle device must also be regularly and continuously deleted. Only the three most recent locations of the vehicle can be stored to determine the vehicle's direction and form the MSD message. The delegated regulation (EU) 2015/758 has since been amended twice. However, the aforementioned points are still included in the current version of the regulation.

Rights of data subjects and informing data subjects

The drivers and passengers of vehicles do not always receive sufficient information about the processing of data in or through connected vehicles. In some cases, this information may only be provided to the owner of the vehicle, who may not be the driver. During the vehicle’s lifecycle, a vehicle may have multiple owners, making it difficult to ensure that every data subject is properly informed.

The regulation on the eCall system (EU) 2015/758 requires manufacturers to provide clear and comprehensive information on how the eCall vehicle device processes personal data along with the vehicle manual. This information must be given in the manual separately for the 112-based eCall vehicle system and any eCall systems supported by third-party services before the use of the system. The user must be reminded of what data is collected and that the system is always active by default. The user must also be informed that the vehicle is not continuously monitored and that their data will only be shared in emergencies.

The user must also be informed of the rights of data subjects. It should be noted that the processing is based on a legal obligation, meaning that the right to object and the right to data portability do not apply in the context of the eCall system. (European Data Protection Board 2021, 32).

Reception and security of eCall messages

The data from the eCall vehicle device must not be shared outside the vehicle device until it is activated. Immediately after activation, the eCall in-vehicle system establishes a voice connection between the vehicle and the emergency response centre and sends the minimum set of data (MSD) from the eCall system to the emergency response centre. The user in the vehicle can manually activate the eCall vehicle device. Activation can also occur automatically when sensors in the vehicle detect an accident.

Data sent through the 112-based eCall service and processed by the emergency response centre may only be transferred to other authorities and other specified service partners in the event of an emergency, and this process is subject to specified conditions. Data processed by the 112-based eCall emergency response service may not be transferred to other third parties without the explicit prior consent of the data subject.

The delegated regulation on the eCall system (EU) 2015/758 defines the requirements for technologies included in the eCall emergency call service that enhance privacy protection. This is considered essential to provide users with appropriate privacy protection and necessary guarantees to prevent surveillance and misuse. Additionally, manufacturers should ensure that the 112-based eCall emergency call service, as well as all other eCall systems offered by third-party services or value-added services, are designed to make data exchange between these systems impossible.

For emergency response centres, member states should ensure that personal data is protected from misuse, including unauthorized access, modification, or loss. Furthermore, it is important that the protocols for the storage, retention period, processing, and protection of personal data are at an appropriate level and strictly followed.

8.2.7 Conclusions on the requirements

Despite the fate of the C-ITS regulation proposal, the development has continued, and, for example, the EU CCMS has yielded several concrete results. At the EU level, data management and data protection have been developed extensively in recent years, but legislation on the specific issues of C-ITS messages remains inadequate. The most significant shortcoming is the lack of clear legal grounds for processing. In the case of C-ITS messages, finding an unambiguous solution to this issue can be challenging, except by imposing a statutory obligation as the basis for processing, or at least by specifying a legal reason that provides for using the public interest as a processing basis. As for the eCall system, the matter has been resolved by stipulating a statutory obligation. The contradictory nature of the requirements is exemplified by the fact that vehicle manufacturers, who collect extensive data on the vehicles they sell and, on their owners, do so based on legitimate interest.

In 2017, WP29 was already drawing attention to other shortcomings in the privacy protection of the C-ITS system. According to WP29, the data protection impact assessment should be prescribed during the legislative process to clarify any risks and mitigation measures from the outset. Additionally, the statement calls for legislation on the legal processing of location data in context of C-ITS applications. There are also several requirements concerning data quality, making vehicle tracking more difficult through technical means, and message-specific data retention times.

The adoption of C-ITS messages is complicated by the lack of specifications, especially regarding the long-range data transmission solution and hybrid environments defined in the C-Roads profile specifications. The C-Roads profile specifications remain incomplete in these respects. The entire trust model does not even cover the key part of long-range communications, i.e. the transmission of messages on mobile networks between the central C-ITS station and vehicles.

In this respect, the formation of personal data depends on the selected mobile technology.

The development of pseudonymisation has advanced to the point where many of the requirements concerning the validity and rotation of certificates have been met. In terms of risk management, approaches such as limiting the retention period of V2I messages containing personal data to 5 minutes makes it more difficult to track users. However, pseudonymization does not guarantee data anonymity, and the possibility of data linkage opens almost endless opportunities for the formation of personal data. Continuous improvement in line with risk management and management system methods is necessary.

A delegated regulation covering C-ITS messages is needed. Uncertainty due to the discrepancies between old official statements, raised issues, and implemented improvements creates doubt about the ability to implement GDPR-compliant data protection. This situation is further exacerbated by, for example, the wide-ranging ways in which car manufacturers collect data on vehicles, the progress made in implementing the SRTI and RTTI regulations, and the continuing investments in C-ITS in several countries. The statements highlight fundamental issues related to location data, the grounds for processing, and the rights of data subjects. For example, car manufacturers collect a wide range of vehicle-related personal data citing legitimate interest, even though the statements advocate for obtaining quality consent from drivers.

8.3 Personal data in C-ITS messages

C-ITS services consist of a wide range of different use cases and various types of information are transmitted within them. C-ITS message profiles have been established for the transmission of data within services. By examining message profiles, it is possible to determine if personal data is being transmitted within them. This chapter examines the data content transmitted in different C-ITS message profiles according to the various C-Roads Platform profile specifications and whether the content may include personal data.

Chapter 6.2.2 describes the typical structure of C-ITS messages. The main components of the message structure are:

- The ETSI security envelope, within which the actual information content (payload) of the signed C-ITS message is transmitted.
- **Short-range C-ITS message.** The message comprises a GeoNet Basic Header and contains information for the basic routing and handling of the message. The contents of C-ITS messages are signed only. This signature ensures the integrity and immutability of the message but does not encrypt the message contents.
- **TLS security envelope for long-range communication.** The TLS protocol forms a security-protecting envelope for the short-range messages in IP-based long-range data transmission. It offers encryption, message integrity verification, and authentication for communication.

8.3.1 Personal data subject to the GDPR in C-ITS messages

According to the EU General Data Protection Regulation (GDPR), personal data refers to any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, a network identification information, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the person.

The GDPR also classifies profiling as personal data, as it is based on the use of personal data. Profiling means any automatic processing of personal data used to assess certain personal characteristics of a natural person, particularly analysing or predicting traits linked to the person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

In C-ITS messages, personal data is assessed to arise in the following ways (Maerivoet & Ons 2023, 66):

Vehicle characteristics and states: location and movement data (coordinates, speeds, direction, accelerations, decelerations, etc.) can be used to reveal the location of a person’s home or workplace. This data may indicate daily routines, the routes they use, and their departure and arrival times. A person’s driving style may be a unique identifier similar to a fingerprint or the way they walk. It may also indicate a person’s risk tolerance or aggressive driving behaviour, which may be of interest to the authorities or insurance companies. Vehicle size and type may reflect personal choices, economic situation, and lifestyle.

Vehicle and device identifiers: may enable linking temporary ID identifiers to permanent identifiers like a registration number, thereby connecting to the owner's personal data. The repeated movement of multiple vehicles together may indicate relationships between individuals.

Time data: message generation times may correlate with personal schedules, thus revealing the person’s working hours, leisure activities, and participation in events or social gatherings.

Intersection and road segment data: can indicate used roads and lanes, forming location-like information about vehicle movements.

It is also crucial to note that personal data is, by definition, information that can be associated with an individual, possibly through additional data. Such extra information is available to car manufacturers or telecommunications operators. An extreme example of personal data formation would be as follows. A vehicle's mobile connection shares WiFi used to distribute copyright-protected material. Copyright holders' representatives are entitled to obtain user information of the corresponding IP address from the Internet service provider through legal proceedings, connecting the IP address to the defendant's identification number. This example highlights pseudonymization's shortcomings as a risk management method. Only anonymization, the removal of personal data, offers a way to release obligations under GDPR, which is practically challenging.

The definition of personal data must also be assessed from the perspective of who considers the same information personal data and who does not. The EU's delegated regulation on road safety data, the SRTI regulation (EU) 2013/886, provides a good example. Data types under the SRTI regulation are V2I information collected from vehicles and contain personal data. Typically, data is collected by car manufacturers, who are data controllers and describe personal data processing in a privacy statement. According to the SRTI regulation, these data must also be collected into a national access point (NAP), executed by means defined by the EU's collaborative body Data for Road Safety (DfRS). DfRS states in its privacy policy (Data for Road Safety, 2021) that they receive only anonymized data from vehicles under agreements with car manufacturers, making tracing single vehicle data impossible. Therefore, DfRS utilizes only anonymized data and does not process personal data.

8.3.2 Personal data contained in different C-ITS messages (Payload)

Based on the above, it is possible to assess the personal data contained in different types of C-ITS messages. The C-ITS message profile data content is transmitted as a signed entity within the ETSI security envelope. This data content is common to messages used for short and long-range communication. Table 14 below presents the data content of different C-ITS message types (C-Roads C-ITS Message Profiles 2023), which may include personal data.

Table 14. Potential personal data contained in different types of C-ITS messages.

C-ITS message profile	Examples of data content that may contain personal data
DENM: Decentralized Environmental Notification Message	In the DENM message profile, Hazardous Location Notification (HLN) and Road Works Warning (RWW) messages are transmitted to warn about hazardous events or maintenance work on the road network. These messages are typically I2V (Infrastructure-to-Vehicle) messages, so no personal data is generated within these messages. Personal data may be created by road operator vehicles involved in maintenance work (V2I). **actionID**: a unique identifier for the message contains information about the C-ITS station (e.g. the identification number of the roadwork vehicle) that generated the message. **detectionTime, referenceTime**: exact time of the detection. **eventPosition, lanePosition**: precise spatial information (longitude, latitude and height coordinates) about an obstacle, event, or condition on the road. **eventSpeed**: the movement speed of the object. **stationType**: indicates the type of C-ITS station (e.g. roadside station, fixed or mobile) or, in the case of a vehicle, the registered vehicle type. **traces**: provides route points approaching the object or incident. It particularly supports autonomous driving in making safe choices.
IVIM: In-Vehicle Information Message	The IVIM message profile transmits In-Vehicle Signage and Automated Vehicle Guidance messages. These messages can, for example, inform drivers about traffic signs or assist automated vehicles in making decisions preferred by the road operator. The messages are typically I2V messages and do not contain personal data. **timestamp**: time of message generation. **referencePosition, zone**: location and area information. **RoadConfiguration, roadType, laneConfiguration, LaneInformation**: provides detailed information about the lanes in the area. **code**: traffic sign code according to ISO 14823 standard **TextContainer**: all free text information related to the traffic sign. **direction**: directional impact of the traffic sign **allowedSaeAutomationLevels**: permitted SAE automation levels. **PlatooningRule**: information about the allowance of vehicle platooning, the number of vehicles involved, speed, distances, and length of the platoon.

C-ITS message profile	Examples of data content that may contain personal data
SPATEM, MAPEM:	In the MAPEM profile, intersection identification and precise location data are transmitted, including intersection topology and lane information. SPATEM messages convey traffic light status information. These messages are typically I2V messages. **IntersectionGeometry and RoadSegment**: defines the precise intersection geometry (number of lanes, traffic light locations, crosswalks, etc.) and road segments outside intersection areas. This information can be linked with, for example, the real-time data generated by vehicle CAM messages. **RegulatorySpeedLimit and AdvisorySpeed**: defines the speed limit and recommended speed when approaching an intersection. **GenericLane and NodeXY**: lane-level geometric and functional details in intersections and nodes or points in lane geometry that provide additional context for traffic arrangements at intersections or other critical points. **IntersectionState**: traffic light status information and timing details for intersections. **MovementState**: more detailed information on the timing of an individual traffic light signal group and the recommended approach speed.
SREM, SSEM SREM (Signal Request Extended Message) SSEM (Signal Status Extended Message)	SREM and SSEM message profiles are used for prioritizing public transport and emergency vehicles at traffic light-controlled intersections. These messages are typically V2I messages. **requestor**: may include identifiers from the party requesting the priority of a signal (e.g. emergency vehicle, public transport). **SignalRequestPackage**: contains information about requested movement through intersections, which can be utilized, for instance, to trace the movement of a specific vehicle at an intersection. **SignalStatus, signalStatusPackage**: describes the response to priority requests and possibly logs interaction data and results concerning vehicles or requestors.
CAM Cooperative Awareness Message	CAM messages provide vehicle or event data to the transport infrastructure (V2I). Data can also be transmitted from one vehicle to another (V2V), but this has not yet been included in the specification. **Station ID**: the unique identifier of a C-ITS station. **Reference Position**: precise location data of the vehicle. **Speed and Heading**: the speed and direction of the vehicle.

	Vehicle Length, Role and Type: information about the vehicle type, trailers, dimensions, role, and e.g., the use of sirens. **Timestamp**: time stamp of the data.
C-ITS message profile	**Examples of data content that may contain personal data**
CPM Collective Perception Message	CPM messages provide information on objects detected by vehicle sensors for other road users and traffic infrastructure. **Originating ITS-S Information**: contains information about the sending vehicle or other C-ITS stations. **Sensor Information**: contains information about the configuration and features of the sensors in use. **Detected Objects**: dynamic information about objects detected in the environment, including the object ID, location, speed, and classification. **Timestamp and Positional Data**: observation time and location of the object.

8.3.3 *Protection of privacy in long-range communication*

The privacy requirements for C-ITS long-range data communication solutions have been carefully considered, but certain challenges remain. Pseudonymization and regular changing of identifiers reduce tracking possibilities over the long term and are a primary method for mitigating privacy-related risks. Information identifying individuals is generally retained for only short durations, typically up to five minutes, to maximize data anonymity. Additionally, security mechanisms such as certificates and encryption (ETSI TS 103 097) protect the integrity and authenticity of messages.

Despite this, specific privacy concerns persist, particularly related to vehicle traceability despite pseudonymization and the integration of networked vehicle systems. This highlights the need for further assessment and potential regulatory changes as technology evolves, emphasizing a balance between the advantages of C-ITS services and privacy protection requirements. Existing methods provide a strong foundation, but ongoing updates and improvements are necessary to address new privacy challenges specifically arising from long-range data transmission.

C-ITS makes use of IP-based communication for long-range communication solution, especially between back-end systems and in infrastructure-to-vehicle (I2V) information services. It allows for the controlled sharing of data, but it also includes certain privacy issues. By combining other datasets, IP addresses can be linked to C-ITS stations and from there to vehicles and persons, or directly to natural persons.

In C-ITS systems, IP-based communication is used for long-range data communication, particularly between back-end systems and infrastructure and vehicle data services (I2V). This enables controlled data sharing, but certain data protection issues are associated with it. IP addresses can be linked to C-ITS stations, and thus to vehicles and individuals, or directly to natural persons by combining them with other data sets.

Pseudonymized identifiers enhance privacy protection, but the risk of identifying individuals remains if the entity attempting identification has sufficient additional information from external sources outside C-ITS services. Retention practices for data generated in C-ITS services instruct that no information enabling individual identification, such as certificates and identifiers attached to C-ITS messages, should be retained for more than five minutes to maintain data anonymity. The possibility of privacy breaches resulting from tracking or unauthorized data use is a recognized concern, addressed in system design through continuous pseudonym changes and strict data retention practices.

In long-range data transmission solutions, C-ITS messages are transmitted in an IP-based network utilizing encryption provided by the TLS protocol. The solution is described in detail in section 6.3. The PKI signature is encrypted within the TLS protocol security envelope. Message transmission in an IP-based network enables controlled and secure data sharing using X.509 certificates and the AMQP protocol for message routing. This minimizes opportunities for unauthorized data use or external entities to leverage the message data content for tracking C-ITS service users. While pseudonymous identifiers can be used to improve privacy, IP-based communication does not completely eliminate privacy risks, as pseudonyms can still potentially be connected to individuals if additional information is available. The C-ITS system is designed to reduce these risks by frequently changing pseudonyms and limiting personal data retention to very short durations.

In communication between C-ITS central stations, signatures in accordance with the EU's C-ITS security credential management system (EU CCMS) are used. The C-Roads profile specifications do not yet address how IP-based I2V or V2I messages are transmitted between the end-user and C-ITS central station, but V2I messages almost invariably transmit time and location data. On the other hand, I2V messages must be able to be targeted via the IP-based network to the recipient's mobile device, so in long-range data transmission solutions, the content of messages should be treated as personal data.

Table 15 compares the personal data contained in different types of C-ITS messages (in short- and long-range communication solutions), and the impact that the direction of the messages (I2V and V2I) has on the formation of personal data. V2V messages have also been considered in DENMs. To clarify, data is considered personal data only when it can be linked to a natural person. Therefore, a vehicle’s time and location data alone is not personal data if it cannot be linked to a natural person. Linking requires additional information, so the table uses the expression *‘May generate personal data’*.

Table 15. Personal data in different types of C-ITS messages (short- and long-range communications), and the impact of the direction of messages (I2V and V2I) on the formation of personal data. V2V messages have been considered in DENMs.

C-ITS message	**V2I (Vehicle-to-Infra)**		**I2V (Infra-to-Vehicle)**	
	Short range	**Long range**	**Short range**	**Long range**
DENM (Hazardous Location Notification & Road Works Warning)	Not used in V2I messages. NOTE! **V2V messages**: unique identifier and accurate spatial data → **May generate personal data.**	Not used in V2I messages. NOTE! **V2V messages**: unique identifier and accurate spatial data → **May generate personal data.**	According to C-Roads Platform definition → **No personal data**	Message content: not personal data. Signature: not personal data. Telecommunications operator knows the location of the subscription, so by combining → **May generate personal data.**
IVIM (In-Vehicle Signage & Automated Vehicle Guidance)	Not used	Not used	According to C-Roads Platform definition → **No personal data**	Message content: not personal data. Signature: not personal data. Telecommunications operator knows the location of the subscription, so by combining → **May generate personal data.**
SPATEM, MAPEM (Signal phase and timing, traffic light priority, Emergency vehicle priority...)	Not used. Vehicle utilises own spatial data, but the data is not transmitted externally.	Not used. Vehicle utilises own spatial data, but the data is not transmitted externally.	According to C-Roads Platform definition → **No personal data**	Message content: not personal data. Signature: not personal data. Telecommunications operator knows the location of the subscription, so by combining → **May generate personal data.**
SSEM, SREM	Prioritised vehicle sends a priority request. Contains time and spatial data on the vehicle. → **May generate personal data.** Max retention time 5 min.	Prioritised vehicle sends a priority request. Contains time and spatial data on the vehicle → **May generate personal data.** Max retention time 5 min.	According to C-Roads Platform definition → **No personal data**	Message content: not personal data. Signature: not personal data. Telecommunications operator knows the location of the subscription, so by combining → **May generate personal data.**

C-ITS message	V2I (Vehicle-to-Infra)		I2V (Infra-to-Vehicle)	
	Short range	**Long range**	**Short range**	**Long range**
CAM (Probe Vehicle Data, Vehicle data collection, Event data collection)	V2I data. V2V data not yet defined. Versatile information about the vehicle and its location is transmitted. → **May generate personal data.** Max retention time 5 min.	V2I data. V2V data not yet defined. Versatile information about the vehicle and its location is transmitted. → **May generate personal data.** Max retention time 5 min.	Not used	Not used
CPM	V2I data. V2V data not yet defined. Versatile information about the vehicle and its location is transmitted. → **May generate personal data.** Max retention time 5 min.	V2I data. V2V data not yet defined. Versatile information about the vehicle and its location is transmitted. → **May generate personal data.** Max retention time 5 min.	Not used	Not used

8.3.4 *Summary of personal data contained in C-ITS messages*

C-ITS stations typically include their own unique identifiers in their messages. A vehicle can act as a C-ITS station, and when it sends data, its unique identifier will also be included in its messages. In line with the analysis above, these identifiers – and C-ITS messages in general – do not contain data that can be defined as personal data, such as information on the driver, street address, registration number, or vehicle VIN code. Furthermore, specific personal group information (ethnic origin, religion, health, etc.) is not transmitted.

Various time and location data, pseudonymized identifiers used in communication between C-ITS stations, and IP addresses are transmitted quite comprehensively. C-ITS messages conforming to the EU CCMS are signed using the public key method. The use of public key method signatures in C-ITS does not make messages anonymous, as the certificates used in these signatures can still be associated with certain users or vehicles using the information provided the Authorisation Authorities (AA) operating under the Enrolment Authority (EA).

C-ITS systems have been designed in a way that their service users cannot be traced. To prevent tracing, these systems use short-term, frequently changing authorization tickets and limit the retention of pseudonymised data to very short periods. This approach reduces the risk of long-term monitoring and is based on the principles of privacy. Although pseudonymity does not guarantee full anonymity, it significantly limits the ability to track and link messages to individual users without additional information, thereby complying with the GDPR’s requirements for the personal data protection.

The structure of messages used in short- and long-range communication is described in more detail in Chapter 6.3.1. Short-range communications can be sent and received by anyone on the given frequency band. The time or spatial data contained in short-range I2V messages does not in itself generate personal data, because the sender cannot identify the recipient. In communications from C-ITS roadside stations and central stations to vehicles and road users, data protection is not considered an important issue, as I2V-type services do not process personal data (C-ITS Security & Governance, 2023, 15).

Using a certificate signed with the public key method, especially in V2I messages, may change this situation. This certificate is pseudonymised data, and thus the recipient can be identified with the help of additional information. For example, in short-range communication, V2I messages (e.g. Probe Vehicle Data, PVD) transmit vehicle data to other vehicles and infrastructure, which can possibly result in the generation of personal data. In addition to the certificate, other information contained in C-ITS messages could also be used to identify C-ITS stations. For example, MAC addresses included in the IEEE 802.11p framework, may be such information.

In designing the C-ITS system, GDPR and privacy protection have been taken seriously, and its principles have been widely incorporated into the system's operational principles. Pseudonymisation is a key strategy for mitigating privacy risks, as it involves regularly changing user identities, thereby reducing the potential for long-term monitoring. C-ITS messages can be said to adhere to GDPR privacy principles, but inherently, particularly transmitted V2I data is personal data and should be treated as such.

8.4 Data and privacy protection in the Finnish implementation model

8.4.1 Roles of authorities in the deployment and use of C-ITS services

In the publication by Traficom “*Viranomaisten roolit vuorovaikutteisten älykkäiden liikennejärjestelmien (C-ITS) palveluiden käyttöönotossa ja operatiivisessa käytössä*” (“The roles of the authorities in the implementation and operational use of Cooperative Intelligent Transport Systems (C-ITS) services”, Kotilainen et al. 2023) the roles of authorities in the deployment and operational use of C-ITS services in Finland are discussed. The report utilizes the architectural description of roles and responsibilities related to C-ITS as presented in the C-Roads WG1 working group's report, following the standard ISO TS 17427. The report emphasizes a well-defined division of roles among authorities and other stakeholders in various tasks.

In the proposed arrangement, Traficom will act as the key market surveillance authority responsible for assessing the conformity of C-ITS stations and supervising safety in cooperation with the Finnish Safety and Chemicals Agency (TUKES). The Finnish Transport Infrastructure Agency and Finnish municipalities will act as owners and operators of infrastructure, responsible for maintaining communication networks and managing roadside stations, for example. This division of roles is described in more detail in Figure 13.

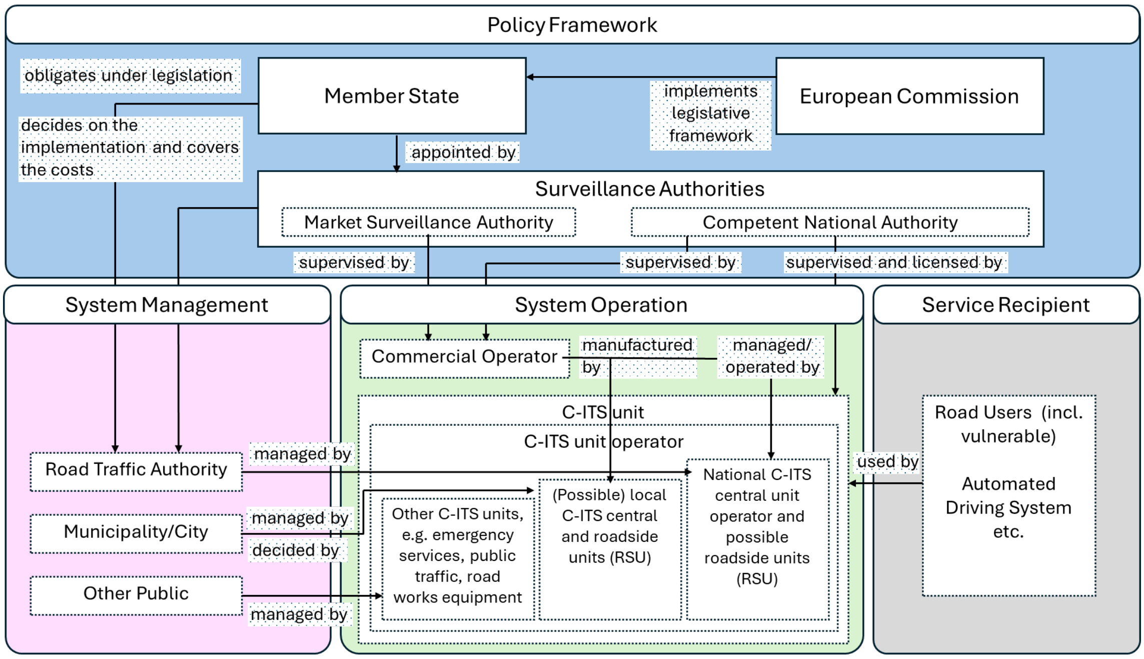

Policy Framework
obligates under legislation
Member State
implements legislative framework
European Commission
decides on the implementation and covers the costs
appointed by
Surveillance Authorities
Market Surveillance Authority
Competent National Authority
supervised by
supervised by
supervised and licensed by
System Management
System Operation
Service Recipient
Commercial Operator
manufactured by
managed/ operated by
C-ITS unit
C-ITS unit operator
Road Traffic Authority
managed by
Municipality/City
managed by
decided by
Other Public
managed by
Other C-ITS units, e.g. emergency services, public traffic, road works equipment
(Possible) local C-ITS central and roadside units (RSU)
National C-ITS central unit operator and possible roadside units (RSU)
used by
Road Users (incl. vulnerable)
Automated Driving System etc.

Figure 13. Division of roles between authorities in the deployment and operational use of C-ITS services in Finland (adapted from Kotilainen et al. 2023).

The report discusses the division of roles for two C-ITS services: (i) Road Works Warning (RWW), with lane closures as a use case, and (ii) Traffic lights, with Signal Phase and Timing Information (SI-SPTI) as its use case.

The operational roles related to the implementation of a lane closure use casea are presented in Figure 14.

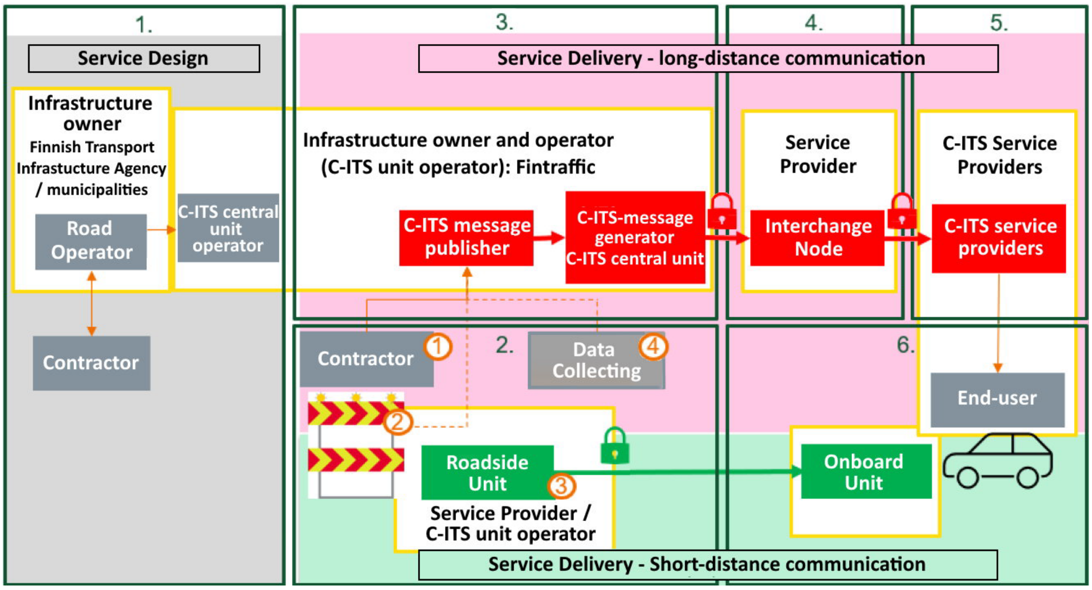

1.
Service Design
Infrastructure owner
Finnish Transport Infrastucture Agency / municipalities
Road Operator
C-ITS central unit operator
Contractor
3.
4.
5.
Service Delivery - long-distance communication
Infrastructure owner and operator (C-ITS unit operator): Fintraffic
C-ITS message publisher
C-ITS-message generator C-ITS central unit
Service Provider
Interchange Node
C-ITS Service Providers
C-ITS service providers
Contractor
1
2.
Data Collecting
4
6.
End-user
2
Roadside Unit
3
Service Provider / C-ITS unit operator
Onboard Unit
Service Delivery - Short-distance communication

Figure 14. Operational roles for closing lanes as part of the Road Works Warning service (Kotilainen et al. 2023).

In the roles shown in Figure 14, the contractor agrees with the infrastructure owner on how the road work warning will be produced. In a long-range communication solution, it is possible to utilise the Road Work Notification service maintained by Fintraffic Tie Oy, or a C-ITS station can be integrated into the road works trailer that communicates its status to the message publisher via a mobile network or a local area network.

The privacy protection in various roles and data communication options (use case: closed lane, I2V) is examined in Table 16.

Table 16. Privacy protection in various roles and data transfer options when handling the closed lane use case of the road works warning service (adapted from Kotilainen et al. 2023).

Task and operator	Short-range communication	Long-range communication
Service definition. Road work client (Finnish Transport Infrastructure Agency, municipality, etc.)	No C-ITS personal data is generated at this stage. The agreement defines, on a case-by-case basis, the data communication method, communication technologies, roadside stations and services, and data quality requirements. Additionally, it is agreed upon who will publish and verify the messages. This stage determines the potential data controller.	
Producer of the road works warning (contractor). The C-ITS station operator is responsible for the security of C-ITS stations.	The contractor uses the C-ITS station integrated into the road works trailer. This involves I2V-type data, no personal data is generated for the sender. The potential for combining this data with, for example, work schedules must be prevented. The C-ITS station operator is subject to ISO 27001/NIS2 obligations.	The contractor uses the C-ITS station integrated into the road works trailer and the mobile network or forwards the data to the publisher (e.g. Fintraffic). This involves I2V-type data, no personal data is generated for the sender. The potential for combining this data with, for example, work schedules must be prevented. The C-ITS station operator is subject to ISO 27001/NIS2 obligations.
Publication and verification of messages (central C-ITS station, national or municipal access point).	Not used.	This involves a central C-ITS station or the national access point (NAP), such as Fintraffic or the contractor. The received data is I2V-type data that does not contain personal data. The potential for combining this data with, for example, work schedules must be prevented. The C-ITS station operator is subject to ISO 27001/NIS2 obligations, and they are responsible for the reliability of the input data.

The operative roles for the **traffic lights** use case are presented in Figure 15, while Table 17 examines the protection of privacy in different roles and data communication options (SI-SPTI messages, I2V).

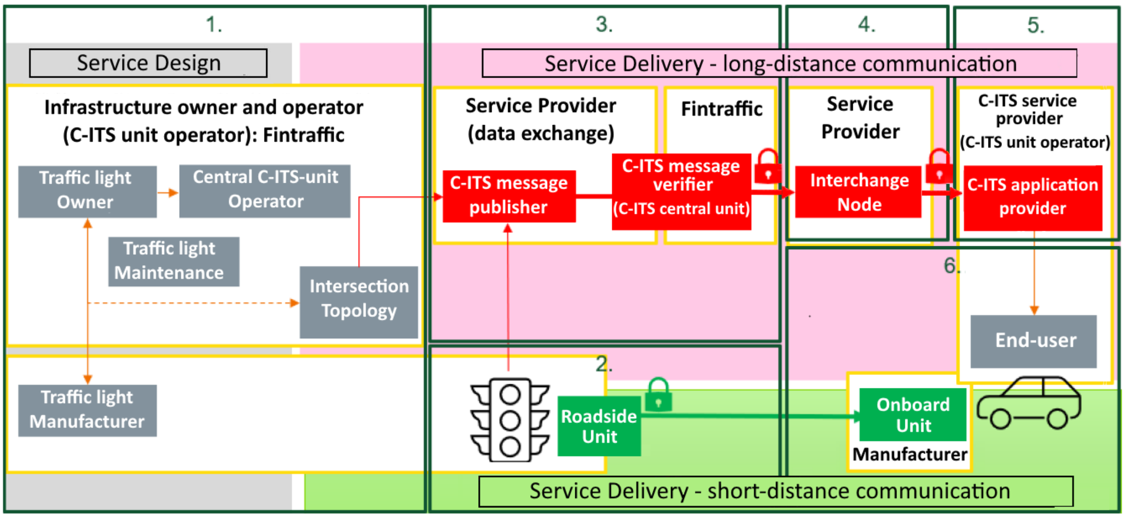


Figure 15. Operational roles in the traffic light (Signal Phase and Timing Information) use case. (adapted from Kotilainen et al. 2023).

The protection of privacy in different roles and data communication options (Signal Phase and Timing Information, I2V) is assessed in Table 17.

Table 17. Privacy protection in different C-ITS roles as part of the tasks and data communication options presented in the report (processing of traffic light SI-SPTI messages).

Task and operator	Short-range communication	Long-range communication
Service definition. Infrastructure owner (Finnish Transport Infrastructure Agency, Fintraffic, ELY Centre, municipality)	No personal data is generated at this stage. During the contracting phase, the owner(s) of the traffic light infrastructure, the traffic light operator, and the operator acting as the C-ITS service provider agree on the data exchange and how the two different types of messages (SPATEM and MAPEM) will be transmitted. The infrastructure owner purchases the equipment from the traffic light manufacturer. During the contracting phase, the parties agree on how SPATEMs and MAPEMs will be transmitted.	
Traffic lights (Traffic light device manufacturer)	The C-ITS station transmits the data as a C-ITS message. The C-ITS station operator (e.g. Fintraffic or the municipality) is responsible for the station’s operation and information security. Traficom is responsible for compliance of radio technology requirements. This involves I2V-type data, no personal data is generated for the sender. The sender signs	The traffic light control unit sends a SPATEM message to the publisher. The message is not yet signed. An I2V-type message does not contain personal data.

	the message and sends it by radio directly to the end-user. The C-ITS station operator is subject to ISO 27001/NIS2 obligations.	
Task and operator	**Short-range communication**	**Long-range communication**
Message publication (Fintraffic, municipality, traffic light manufacturer's system)	Not used.	The message publisher, such as Fintraffic, a municipal access point, or the back-end system of the traffic light manufacturer, sends the SPATEM and MAPEM data forward for signing. The signature and transmission take place in the central C-ITS station and are carried out by, for example, Fintraffic or the traffic light manufacturer. The received traffic light data is I2V-type information which does not contain personal data. The central C-ITS station operator is subject to ISO 27001/NIS2 obligations. It is responsible for the reliability of the input data.

The common roles described for both use cases are presented in Figure 16, while Table 18 examines the privacy protection in these different roles and data communication options.

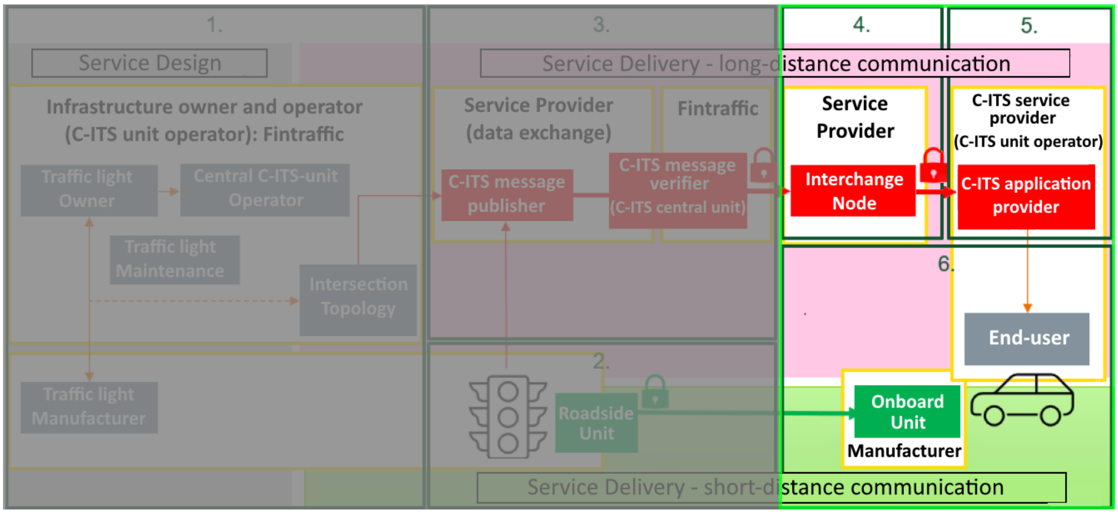

1.
Service Design
Infrastructure owner and operator (C-ITS unit operator): Fintraffic
Traffic light Owner
Central C-ITS-unit Operator
Traffic light Maintenance
Intersection Topology
Traffic light Manufacturer
3.
Service Delivery - long-distance communication
Service Provider (data exchange)
Fintraffic
C-ITS message publisher
C-ITS message verifier (C-ITS central unit)
2.
Roadside Unit
4.
Service Provider
Interchange Node
5.
C-ITS service provider (C-ITS unit operator)
C-ITS application provider
6.
End-user
Onboard Unit
Manufacturer
Service Delivery - short-distance communication

Figure 16. Common operational roles described for both use cases (adapted from Kotilainen et al. 2023).

Table 18. Privacy protection in different C-ITS roles as part of the use cases presented in the report (common activities).

Task and operator	Short-range communication	Long-range communication
Interchange server (Fintraffic, municipality, C-ITS service provider)	Not used	Forwards signed C-ITS messages to C-ITS service providers. Processing is based on the AMQP header. Does not sign messages. The data processed is I2V-type information which does not contain personal data. Possible data combinations with, for example, work schedules must be prevented. ISO 27001 obligations do not apply, but NIS2 directive obligations do.
Private or public C-ITS service provider	Not used	Orders the C-ITS messages used from the area where the service users are moving. Checks the message certificate and transmission rights. Sends the message to the end user using methods according to its own solution and, in this regard, is not part of the EU C-ITS security credential management system (EU CCMS). An I2V-type message itself does not contain personal data, but the service provider has other personal data about its customer, and it acts as the data controller. Commercial operators typically use a legitimate interest (customer relationship) or a contractual relationship as the basis for their processing.
End-user (vehicle driver, automated driving system, unprotected road user)	Vehicle C-ITS station. Checks the message’s certificate. Does not contain personal data. No specific requirements for the end-user.	A method provided by the C-ITS service producer, for example a mobile application. No specific requirements for the end-user.

The C-ITS roles report recommends setting up national-level coordination groups consisting of representatives from the state, municipalities, and private actors. These groups focus on the definition of C-ITS services and the continuous development of these services as technology improves. Additionally, a competent authority is to be proposed as a national authority that grants authorisations to C-ITS stations that can send special messages, such as for emergency vehicles.

If the services are implemented nationally, Fintraffic Tie Oy will have a key role as a central C-ITS station operator, and it will be responsible for publishing and verifying messages. The report emphasises the use of different solutions, such as long and short-range communication and their management through different actors, such as contractors and C-ITS station operators.

Coordination between public authorities, private actors, and end-users will be essential for the overall development and effective and secure monitoring of C-ITS, both at the national and European level.

8.4.2 Supervisory authority

The national data protection supervisory authority is the Data Protection Ombudsman. The Finnish Transport and Communications Agency Traficom acts as the market surveillance authority. Its role is to oversee electronic communications services and transport services in relation to consumer rights and market functionality. Traficom addresses issues such as anti-competitive practices or actions that infringe on consumer rights, but it does not focus on data protection to the same extent as the Data Protection Ombudsman.

8.4.3 Administration and management

Impacts of data protection legislation: In the role of data controller, as support for management and decision-making, there is an obligation to conduct a data protection impact assessment and prepare a record of processing activities. This enables the ability to inform the data subject about the processing of personal data and their rights.

8.4.4 Summary of compliance with data protection and information security requirements in Finland

If C-ITS services are deployed in the manner described in the C-ITS services report on the roles of authorities (Kotilainen et al. 2023) using the described organisations and technologies, Finland will need to implement the following measures to meet the EU’s data protection and information security requirements:

- GDPR-compliant processing of personal data in organisations participating in the transmission and storage of messages, such as Fintraffic, municipalities and private actors.
- C-ITS operators are required to have a certified information security management system according to ISO 27001 (private sector) or apply the requirements of the NIS1 and NIS2 cybersecurity directives (road authorities).

- A national framework for the exchange of verified data between C-ITS stations, in accordance with the EU CCMS described in Chapter 5.
- The security-related assessment and certification of C-ITS stations require a SOG-IS conformity evaluation body. There is no such evaluation body in Finland, but evaluation bodies in other countries in Europe can be used in accordance with the principles of the Mutual Recognition Agreement (MRA).
- A clearer definition of the roles of different authorities, such as Traficom and the Finnish Transport Infrastructure Agency, as well as private actors, such as commercial service providers. There is a need for clear agreements and definitions on how costs and operating responsibilities as well as the ownership, management, and maintenance of infrastructure should be distributed among different actors, especially when services cross national borders.

8.4.5 System operation

Impacts of data protection legislation: actions taken on behalf of the controller as an operator are described in the processor's records of their processing activities. The record serves to inform the data subject about the processing of personal data and their rights.

Where necessary, the processor must assist the controller in carrying out the data protection impact assessment. In addition, the processor must notify the controller of any personal data breaches, ensure adequate data security, perform the necessary data destruction operations, and participate in audits.

8.4.6 End-user

Impact of data protection legislation: the rights of the data subject are fulfilled with measures in place to facilitate their exercise. Based on the data protection impact assessment carried out by the controller, the potential risks to the data subject have been identified, and the data subject should have the opportunity to decide whether to share their personal data with the C-ITS service.

8.5 Summary and recommendations

In C-ITS services, a lot of attention has been paid to the implementation of privacy protection, and despite the absence of a specific C-ITS regulation, C-ITS implementations have started in several EU countries. Nevertheless, it should be noted that issues related to the implementation of the principles of the EU's General Data Protection Regulation (GDPR) and the protection of personal data and privacy have not yet been fully resolved.

8.5.1 Risk management

According to the principles of data protection, the controller must always assess the risks related to the processing of personal data before they begin processing any personal data. The purpose of the data protection impact assessment is to help identify, assess, and manage the risks involved in the processing of personal data. It is intended as a continuous process of risk identification and management.

The EU General Data Protection Regulation (GDPR) does not explicitly require a Transfer Impact Assessment (TIA) as a separate concept, but the EU data protection authorities and the European Data Protection Board (EDPB) have highlighted its importance as part of fulfilling GDPR obligations. Especially in situations where personal data is transferred outside the EU/EEA without an adequacy decision, the TIA is considered a vital part of the introduction of appropriate safeguards and risk management.

In the event of a personal data breach, the controller is obliged to assess the risk level of the event, document it accordingly, and notify the supervisory authority. The data subject must be notified of a personal data breach if it is likely to pose a high risk to their rights and freedoms.

In addition to the privacy and data protection principles, national legislation requires the destruction or pseudonymisation of electronic messages and transmission data. Pseudonymization can reduce risks associated with personal data by modifying personal data with artificial identifiers so that the data cannot be linked to a specific person without additional information.

The data protection assessment and handling process has been defined with the help of Section 5.4 (Planning) of the data protection extension ISO/IEC 27701 (PIMS) to the standard for information security management systems (ISMS, ISO/IEC 27001). The data protection assessment and handling process identifies the risks related to the processing of personal data. Section 8 (Operation) of the Information Security Management System is applied to the privacy management system without additional requirements for proper risk management.

Risk management obligations stem from many different sources, which together form a comprehensive framework for the development and maintenance of the data protection practices of organisations. EU data protection legislation imposes obligations on controllers and processors to identify and manage risks related to the processing of personal data. National data protection legislation complements the requirements presented in EU legislation. It can include specific obligations that address the specific data protection or information security needs of the country concerned. Management system standards provide a structural approach to data protection-related risk management, define the processes for identifying, assessing, and managing risks, and present methods for ensuring the adequacy and effectiveness of management methods.

Alongside EU-level and national data protection legislation, standards can provide organisations with concrete processes and tools to meet legislative requirements and continuously improve privacy practices. Risk management requires continuous monitoring, assessment, and improvement. Continuous improvement enables organisations to adapt to changing threats and new data and personal protection requirements.

All these elements support a multi-layered approach to risk management, where EU and national requirements and standards guide the organisations´actions with practical methods. Cooperation and an integrated approach enable the systematic identification, assessment, and management of risks, and help organisations remain compliant.

8.5.2 Deficiencies in national or EU-level regulation

The scope of the network for transmitting C-ITS messages and the amount of personal data to be processed have been highlighted in many contexts as specific issues requiring the development and approval of a delegated C-ITS Regulation. This regulation must also gain the approval of the European Data Protection Board (EDPB). In the absence of legislation on C-ITS and C-ITS services, the situation is contradictory in many respects, and established case law has not been developed. At the time of writing the report, there was no available information on the future processing of the regulation.

Especially for end-users, any grounds for processing that are based on consent, or a contractual basis is difficult to implement for C-ITS messages. A legitimate interest, on the other hand, usually requires case-specific balancing tests and additional protective measures, which is challenging in a wide-ranging national service.

The public interest is a good candidate for a processing basis, especially for the authorities. The use of the public interest should be supported by national or EU legislation, to confirm the necessity of the processing to achieve a specific public interest. This means that the processing must be closely linked to a democratically accepted objective or to the needs of society.

Regarding the grounds for processing, it seems inevitable that the wider implementation of C-ITS services will require the incorporation of grounds related to the public interest (e.g. traffic safety) into legislation. The legislation must clearly define the public interest and how personal data can be processed based on this interest. This may include information on who is responsible for the processing, as well as the limitations of and conditions for the processing. Improving road safety could be used as a public interest, but this must be part of a broader legislative framework that specifies the situations and conditions under which the processing of personal data is permitted to achieve these objectives. This approach is likely feasible. Alternatively, the implementation of C-ITS services could be included as a statutory obligation, which would make it the basis for the processing. Implementing this approach is likely to require broader international cooperation.

It is difficult to inform the users of C-ITS services about how their data is used. The GDPR emphasises transparency and the right of the user to access their data, so it is important to develop the related mechanisms and legislation. In the case of the vehicle emergency call system, i.e. eCall, the issue was resolved by informing the driver in the vehicle’s instruction manual. However, in the case of C-ITS, it has been criticized that this is not sufficient.

Areas for improvement at the national level

Finland should implement several measures to address its legislative shortcomings in C-ITS services. The most essential task is the development of national legislation in line with the forthcoming EU C-ITS Regulation, which will establish uniform rules for the implementation of services at the Member State level. This will require preparing and approving national legislative amendments in Finland in accordance with the ITS Directive (EU 2023/2661) and other EU regulations. In addition, national authorities and ministries should continue to participate actively in EU-level working groups, such as the C-Roads Platform, which aim to harmonise the deployment of C-ITS in the Member States.

Market surveillance and information security laws, such as the provisions under the NIS2 Directive, should be updated to meet evolving security requirements and the challenges posed by new technologies. At the time this report was written, the NIS2 Directive was being discussed by the Finnish Parliament.

Good and effective practices can help to compensate for legislative shortcomings. Strengthening the cooperation between various actors, such as the Finnish Transport Infrastructure Agency, Fintraffic Tie Oy, Traficom, and private service providers, is of vital importance. This cooperation can contribute to clarifying the responsibilities and operating models necessary for the secure and efficient implementation of all C-ITS services.

The legislation and technology in the sector are developing at a rapid pace. To ensure that the regulation of C-ITS services is always up-to-date and to the level of both national and EU requirements, the continuous implementation of impact assessments and regulatory adaptations should be integrated into the national legislative process. The related impacts should be assessed both in the preparation phase of new laws and in the monitoring of laws that have entered into force.

8.5.3 Deficiencies in C-Roads Platform specifications

Integrating various communication technologies (such as short- and long-range data communication solutions and hybrid environments) into a seamless and GDPR-compliant system requires additional specifications in the guidance and legislation concerning the privacy protection of different messages. Clarity is needed for considering mobile network connections that fall outside the EU trust model regarding the overall privacy protection of the C-ITS system.

PKI authentication and pseudonymization are in use, but dynamic switching of certificates might be insufficient. This means that pseudonyms may not change frequently enough, potentially leading to user traceability over a longer period. In practice, it may be difficult to monitor the five-minute retention period of certificates. In short-range communications, anyone can receive unencrypted messages sent over the ITS-G5 band. In long-range communication, on the other hand, there may be a large number of service providers capable of ordering messages or that otherwise have access to them. Supplementing PKI certificates with advanced cryptographic methods (e.g. Group Signatures) could be a good technical addition to preventing any unnecessary accumulation of personal data.

Defining and managing data retention periods may be absent or vague, leading to unnecessary data retention and thus violating GDPR. Clear definition of retention periods helps data controllers improve their operations and comply with GDPR requirements.

Addressing the above-mentioned shortcomings requires development work by the C-Roads collaboration bodies, but also a continuous need to assess the development of technology and regulations.

8.5.4 *Privacy protection is a balance between risks and benefits*

C-ITS services aim to balance the risks associated with privacy protection and the benefits achieved through various mechanisms. C-ITS messages are designed to protect personal data while enabling effective communication between vehicles and between vehicles and infrastructure.

Privacy risks are related to user tracking and the combination of location data. The location data contained in C-ITS messages can reveal the precise location of an individual at a given moment, potentially leading to personal tracking. Continuous collection of location data can reveal movement patterns, the address of a workplace or home, and frequently visited places. Processing such data can lead to unwelcome surveillance or profiling. Particularly when location data is combined with other personal information, the risk to privacy protection can significantly increase.

When using pseudonymised identifiers, there is a risk that sufficient additional information may enable the identification of individual users. It is also possible that personal data is retained longer due to inadequate practices or local laws, which may conflict with privacy protection principles.

C-ITS services are expected to achieve numerous benefits. Traffic becomes safer, smoother, and with lower emissions. It enables technological advancement, for instance, better integration of automated vehicles into the traffic system. C-ITS facilitates cross-border interoperability in international transport and logistics.

The improvement of safety and efficiency enabled by C-ITS justifies the management of privacy risks, by ensuring that personal data is processed carefully in accordance with the regulatory requirements. These measures demonstrate that C-ITS service definitions have sought a balance between privacy protection and service functionality, even though complete anonymization is not possible. The clear aim has been to protect personal data in compliance with GDPR requirements, but known shortcomings related to technology, legislation, and experience in service implementation and regulation require ongoing surveillance of the situation.

9 Capabilities and potential of mobile network technology

9.1 Impact of a communication solution on the implementation of C-ITS services

Long-range communication solution based on mobile networks has, as they have evolved, emerged as a viable alternative to short-range broadcast-based solutions for implementing C-ITS services.

In a study commissioned by Traficom (Kilpiö et al. 2024), the following were identified as arguments for favouring the use of mobile network technology: the wide coverage for commercial mobile networks, the fact that these networks are continuously maintained and developed, and their sufficient performance characteristics for C-ITS services, including adequate capacity and low latency.

From the technical standpoint, it can be argued that it has been justified to begin developing and standardising solutions based on mobile network technologies as part of the broader C-ITS ecosystem (commercial motivations are excluded from this examination). The fixed part of the Internet used in long-range communication solutions shares similar characteristics with mobile networks: wide coverage, built-in maintenance and development, and strong performance.

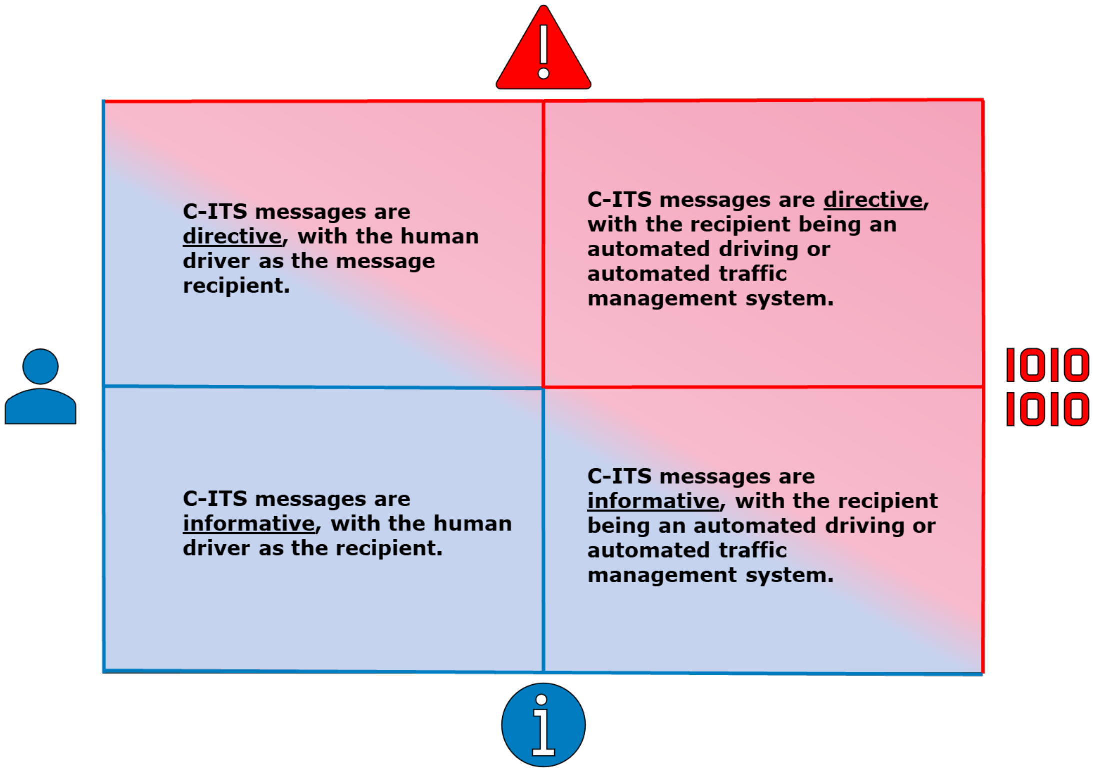
Another study commissioned by Traficom on the piloting of C-ITS services (Kynsijärvi et al. 2024) found that, from the perspective of the network platform, long-range communication solutions utilising commercial mobile networks and the public Internet currently operate without any guaranteed network performance – commonly referred to as a "best-effort" environment. However, based on the performance tests carried out within the project, the study recommended that informative C-ITS services can be implemented in such best-effort public network environments. At the same time, the study emphasized that as the CCAM (Cooperative Connected Automated Mobility) domain evolves, and current or future C-ITS messages are used for more critical traffic management purposes – or even influence vehicle driving behaviour – it will become increasingly important to ensure an appropriate service level (Service Level Agreement, SLA) for such communication and the associated centralized services.

Similarly, expert interviews (Swarco interview, 2024) highlighted a comparable division between safety-critical applications and those aimed at improving traffic efficiency and comfort within C-ITS services. The use of mobile networks for long-range communication was considered challenging for safety-critical application. The interviews also emphasized a lack of a service level agreement (SLA) concerning network quality of service, as well as insufficient specifications related to network components.

Due to the perspectives mentioned above, it may be justified to consider C-ITS services along two different axes: on concerning who utilizes the messages – whether a human driver or an automated driving or traffic management system responsible for dynamic driving tasks – and the other concerning the nature of the messages – whether they are informative or involve direct influence on vehicle behaviour, as illustrated in Figure 17.

A cooperative driving use case involving V2X services — which also include C-ITS services — as described above, has been identified as a potential future application by the CAR 2 CAR Communication Consortium. In such a scenario, vehicles could share information about their intentions with one another, thereby facilitating the coordination of automated vehicles in various traffic situations (CAR 2 CAR Communication Consortium, 2019).

The link between C-ITS and CCAM development has also been recognised in the CCAM Partnership programme (CCAM Partnership, 2023), where public and private sector stakeholders aim to align their research and development efforts to accelerate the deployment of CCAM technologies and services across Europe. The programme is guided by a Strategic Research and Innovation Agenda (SRIA), a multi-year roadmap. This roadmap identifies C-ITS development as a key enabling activity in the creation of the digital infrastructure needed for CCAM. In addition to informative use cases for C-ITS messages, the roadmap also recognises applications involving direct influence on vehicle behaviour, such as supporting in overtaking or intersection scenarios (CCAM Partnership, 2023).



C-ITS messages are directive, with the human driver as the message recipient.

C-ITS messages are directive, with the recipient being an automated driving or automated traffic management system.

C-ITS messages are informative, with the human driver as the recipient.

C-ITS messages are informative, with the recipient being an automated driving or automated traffic management system.

Figure 17. Classification of C-ITS services

As illustrated in Figure 17, the first category (top-left corner) represents a case where C-ITS messages involve direct influence on vehicle behaviour, and the recipient is a human driver. In this situation, C-ITS messages provide traffic management-related information — such as speed limits or traffic signal status — that the driver is expected to obey. The information conveyed by C-ITS messages is comparable to that provided by traditional traffic signs and traffic control devices. In this context, the timeliness and reliability of C-ITS messages are particularly important.

In the second category (bottom-left corner), C-ITS messages are informative, and the recipient is a human driver. Here, the messages provide information about the traffic environment and situation, enabling the driver to adjust, for example, their speed or route choice accordingly. C-ITS messages may also warn of unexpected or time-critical situations — such as a broken-down vehicle on a motorway or a vehicle running a red light — that require immediate driver response. Failure to respond to such warnings may increase the likelihood or severity of an accident. The timeliness and reliability of C-ITS messages are especially critical in this context, with transmission latency becoming a significant factor when warning of nearby, time-sensitive hazards.

In the third category (top-right corner), C-ITS messages are also used in applications involving direct influence on vehicle behaviour, but the recipient being an automated driving or traffic management system. Although vehicles perceive their surroundings using onboard sensors and typically apply redundancy in decision-making, control information delivered via C-ITS messages can influence vehicle behaviour. An example of such a scenario is the future use case of cooperative driving proposed by the CAR 2 CAR Communication Consortium — such as merging onto a road or navigating an intersection. These applications are part of a longer-term development roadmap and raise numerous unresolved issues, particularly regarding liability.

Additionally, an automated traffic management system may carry out traffic control actions — such as providing priority for public transport or controlling traffic lights — based directly on information provided by C-ITS messages (e.g., CAM messages transmitted by vehicles). In these cases, the quality, reliability, and latency of C-ITS messages are critical to ensuring safe operation.

In the fourth category (bottom-right corner), C-ITS messages are informative, and the recipient is an automated driving or traffic management system. These messages provide vehicles with an extended digital horizon, offering information beyond the range of their onboard sensors. Vehicles use this data to cross-verify their own sensor-based observations — functioning as a parallel fallback system — but do not rely solely on these messages to make operational decisions.

Similarly, information provided by C-ITS messages can be utilised in automated traffic management systems. However, in critical situations, a human traffic operator may still make the final decision on the necessary actions.

Although this study does not take a position on the suitability of different communication technologies for implementing various C-ITS services (as defined in the limitations of this work, see Chapter 1.2), the categorisation outlined above nevertheless provides grounds for further consideration of this perspective. The topic is further discussed in the following subsections from the viewpoint of network technology development and general network architectural design relevant to the implementation of C-ITS services. These perspectives are based on the working group's expertise in the use of telecommunications technologies in large-scale WAN (Wide Area Network) solutions and as part of IoT (Internet of Things) systems.

9.2 Differences between short- and long-range communication solutions

It is important to note that, for a long time, the development of C-ITS services was primarily based on short-range solutions and radio technologies, and the influence of this background is still evident in many aspects today. The operational environment based on short-range solutions differs significantly from that of long-range communication environments in terms of telecommunications technology.

In the radio-based implementation of short-range communication, the available communication capacity is fully dedicated to a specific purpose. The radio channel capacity used by C-ITS stations is entirely dedicated to C-ITS services, and there is no competition for this communication capacity. However, even this implementation model does not guarantee a specific service level. If the radio channel becomes congested, delays in packet transmission may occur, and in the worst case, message delivery may fail.

From an information security perspective, radio technology is inherently very open. Roadside C-ITS stations communicate with their environment in a beacon-like manner (broadcast), and anyone who "tunes their receiver" to the same frequency can listen. In addition to listening, virtually any party with suitable equipment and programming skills can also transmit messages. In such an environment, the C-ITS Security Credential Management System (EU CCMS) provides a robust level of security. It ensures that message recipients can verify that a message was sent by a trusted entity (authentication) and check the integrity of each received packet to ensure that the message has not been manipulated in transit.

From an administrative perspective, deploying a short-range communication environment is particularly challenging on urban street networks, which are typically maintained by municipalities. Implementing full network coverage of roadside C-ITS stations along roads and streets is a significant investment—not to mention the costs related to maintenance and lifecycle management (such as field maintenance response times, decentralized spare parts storage, software updates, and hardware replacements due to technological evolution).

The long-range communication option is, in many respects, the opposite from a network perspective; instead of being closed, it is completely open regarding the services transmitted over the network. Long-range communication uses a public consumer mobile network, which then transitions to the fixed network side via the open Internet. The network capacity is shared by countless applications used by consumers and businesses, and the message path from a vehicle or roadside station to the central C-ITS station (for example, a cloud service located in a Microsoft Azure data centre within the EU) may pass through dozens or even hundreds of network devices, none of which are under the control of the party responsible for the operational management of the C-ITS deployment. When used this way, the public network(s) therefore do not provide any form of service level guarantee in terms of capacity or latency for C-ITS services.

From the perspective of information security for long-range communication-based C-ITS solutions, the current EU CCMS is applicable to public network environments. The system provides useful security features even in such open environments. However, this technical implementation also highlights the differing development approaches between short-range and long-range communication solutions. What is well justified in short-range communication may be unnecessary, or at least addressed differently, in long-range communication.

The open IP-based Internet network offers several existing and lighter-weight solutions to handle the same security concerns — reliable user authentication and data encryption. These commonly used public network security mechanisms, such as TLS and X.509, are also employed in long-range communication solutions to complement the measures provided by the EU CCMS, in accordance with the requirements of the C-Roads specifications.

A large-scale deployment of short-range communication-based C-ITS solutions faces challenges primarily related to high construction, maintenance, and operational costs. These systems are also vulnerable to hardware failures. The failure of a single roadside station can regionally disrupt communication between vehicles and infrastructure (though redundancy of stations can mitigate this issue). The radio frequency used is sensitive to physical obstacles between the transmitter and receiver, requiring a line-of-sight connection.

By contrast, long-range communication-based solutions address many of the weaknesses associated with short-range solutions. The network already offers extensive coverage, professional development, and maintenance. Cell sizes are relatively large, with a high likelihood of frequency or base station coverage overlap, and the frequencies used are less sensible to physical obstructions.

From a network performance perspective, both solutions are strong. While short-range communication does not provide as much data capacity as, for example, 5G networks, the capacity is sufficient for C-ITS service needs and is fully dedicated to their use.

9.3 Identified problems in long-range communication solutions

Performance tests on public mobile networks and the Internet have yielded promising results regarding their suitability for C-ITS service implementation (Kynsijärvi et al. 2024). However, a key limitation of these tests lies in their short duration and geographically limited scope. Despite these limitations, the results remain promising. Based on them, it can be stated that these networks generally offer sufficient — and in most cases excellent — performance for C-ITS services.

It is inherently difficult to comprehensively test mobile network performance at scale, as it can vary significantly across different geographical areas — even within the same city — and particularly between countries. Furthermore, the tests conducted so far have not included large-scale trials with high numbers of simultaneous users (although such experiences do exist, for example, in the Dutch C-ITS ecosystem).

Furthermore, even wide network coverage is not absolute; there may still be coverage gaps in locations that are particularly problematic from the perspective of C-ITS system operation.

Factors that may negatively impact the performance of mobile networks include various external influences, such as mass events causing significant user spikes, traffic jams, traffic accident situations, or issues with the operator’s backbone network. The fixed part of the Internet is vulnerable to cyberattack scenarios (e.g., regional or service-specific denial-of-service attacks), hardware failures and cable cuts in network operators' backbone infrastructure, as well as breaks in key global submarine cables.

A particular concern is the vulnerability of services hosted on the Internet to cybersecurity threats. Among these, Distributed Denial of Service (DDoS) attacks represent a significant risk, especially for services with public-facing interfaces in open networks (such as cloud services connected to the public Internet or services hosted in data centres).

The aforementioned challenges of public networks can be considered very fundamental, especially in connection with the implementation of real-time and increasingly security-critical C-ITS services. The development of C-ITS solutions has included considerable efforts to ensure the confidentiality of parties and the integrity of C-ITS messages (EU CCMS). Significant progress has also been made in long-range communication solutions for encrypting sessions between background systems and authenticating parties (C-Roads Platform). However, the development of long-range communication solutions has paid relatively little attention to enhancing the security and service level (SLA) of services connected to networks and the network solutions they use (e.g. closed WANs).

It is very likely that the NIS2 Directive alone will impose significant additional requirements for the development of a pan-European C-ITS system. These requirements specifically target the planning and deployment of the network implementations utilised by C-ITS deployments, as the transport sector is one of the highly critical sectors under the NIS2 Directive. This classification sets specific requirements on the management of technical systems and the cybersecurity on their implementations within the transport sector.

9.4 Development trends

Despite the issues highlighted above concerning long-range communication solutions and their data communication architectures, the information system architecture is, in many respects, also easy to develop.

The role of the mobile network in supporting C-ITS services is currently somewhat more challenging. It is possible to purchase organisation-specific private APN services (Access Point Name) from mobile networks, but these are always operator-specific, and networks do not currently offer application-specific QoS or CoS services (Quality/Class of Service) that could provide a higher level of service for selected applications. Various potential future development proposals to improve the service level of mobile networks, including network slicing, have been presented in more detail in Traficom's previous studies (Kilpiö et al. 2024).

Currently, the Finnish mobile network is predominantly based on 4G and 5G technologies, and this trend is expected to continue in the near future, as 5G deployment has rapidly advanced across Europe in recent years. The European Commission has actively promoted 5G rollout and secured funding for its development. In 2016, the Commission adopted a 5G Action Plan aiming to kick-start 5G deployment in all Member States by 2020 and to ensure uninterrupted coverage in major urban areas and key transport routes by 2025 (EU 2016/588, 2016). Furthermore, the European Digital Compass, published in 2021, set an additional target for full 5G coverage across all populated areas by 2030 (EU 2021/118, 2021). The Commission has also funded 5G development projects along critical transport corridors through the Connecting Europe Facility's digital strand (CEF Digital), supporting infrastructure development and research initiatives (European Commission, 2022). Additionally, investment in future 6G network technology research and development is underway, with related standardisation activities expected to begin in 2025. To facilitate this, the EU established the Smart Networks and Services Joint Undertaking (SNS JU) in 2021 (De Luca 2024).

Benefits of fifth- and sixth-generation wireless network technologies include increased data transfer rates, low latency, and high reliability, all of which enhance the implementation of C-ITS services. An earlier study by Traficom (Kilpiö et al. 2024) identified key performance indicators (KPIs) for the service level of C-ITS services operating over mobile networks. These include availability (network coverage), reliability (packet loss rate), and integrity (upload/download speed and latency). The same study concluded that the currently deployed 4G networks already enable the implementation of C-ITS services from a network technology performance perspective.

In addition to network technology, the system capacity of mobile networks is significantly influenced by the spectrum used in different areas and the network topology. Different frequency bands are suitable for different purposes; lower-frequency, narrower bands achieve greater coverage due to lower radio signal attenuation but offer lower capacity. Conversely, higher-frequency, wider bands provide higher capacity but require a denser base station network.

The study also highlighted a key criticism discussed in Section 9.3: mobile networks are inherently highly dependent on the environment, and poor service levels occur across all domestic operators depending on the deployment and strategy of their local networks. Thus, a central issue is the lack of guaranteed service levels, particularly for safety-critical C-ITS services. Although evolving and future network technologies introduce more advanced mechanisms and new features to improve service levels, the development of network technologies alone does not guarantee specific service levels for C-ITS services.

Nevertheless, it can be assumed that the development of future network technologies and their new features will also support the implementation of C-ITS services using long-range communication solutions. The exact magnitude of these impacts is difficult to assess, as 6G network technology is still in the research and development phase, making its actual performance partly speculative. Moreover, 5G network technology has not yet achieved the required coverage (for example, outside major cities and key transport routes), and ongoing development, innovation, and new standard releases continue in this area as well.

Companies providing communication network solutions and technologies, such as Nokia, have envisioned numerous new use cases especially for 6G, enabling large-scale digital twins and augmented reality applications as extensions of the physical world (Viswanathan & Mogensen, 2023). Considering CCAM applications and the future development of transport, future network technologies will likely enable a significant number of new mobility use cases that could not be supported solely by short-range communication solutions due to their limited capacity. It can be assumed that mobile networks will become increasingly central also from the transport sector perspective in the future.

In any case, from the perspective of C-ITS service deployment, there is no need to wait for the evolution of network technologies, as a large share of C-ITS services can already be covered by current 4G and 5G technologies, provided that occasional regional variations and temporary decreases in service level are accepted. This may require a more detailed, service-specific examination of C-ITS requirements, as proposed in Section 9.1.

There are numerous development measures available for fixed Internet networks. The location of central C-ITS stations within the C-ITS system can be regulated (e.g., restricted to domestic data centres only), and the communication implementation between central C-ITS stations can be carried out through a separately procured closed network solution that guarantees the quality of service for the connections.

If major global cloud services are used as the location for central C-ITS stations, it is also possible to purchase closed, secure communication connections with SLA guarantees for these services.

At the EU level, a closed network environment could be established to form connections between inter-country interchange servers, requiring the interchange servers of each country and organisation to join a Europe-wide C-ITS trust network. This would provide guaranteed service levels (capacity) for connections between interchange servers and allow these services to be separated from the public network, thus protecting them from denial-of-service attacks.

A similar arrangement could also be implemented nationally for central C-ITS stations, offering a guaranteed service level and closed communication between them.

10 National intent for the implementation of C-ITS services

No EU or national regulation obliges Member States to implement C-ITS services or to introduce the related components, such as central stations. However, the revised ITS Directive (EU 2023/2661, 2023) and the delegated regulations under it have introduced certain obligations, with a long-term goal of achieving the large-scale deployment of ITS services across the Member States.

The aim of the revised ITS Directive was to update and extend the scope of the Directive to cover new services and technologies, including C-ITS. In essence, some of the specifications mentioned in the 2019 Delegated Regulation on the deployment of C-ITS (EU C/2019/1789, 2019) have been incorporated into the revised Directive, although it does not represent a direct re-review of the Delegated Regulation rejected in 2019. In other words, the revised ITS Directive takes a much stronger position on the issue and states that C-ITS services represent one of the categories of ITS services, in which case it can be concluded that the regulation and promotion of C-ITS services continues to play an active role at the EU level and on the Commission’s agenda.

This conclusion is also supported by the European Commission Implementing Decision that confirms the working programme of Directive 2010/40/EU for 2024–2028 (C/2024/6798, 2024), in which C-ITS has also been taken into account as a separate action. This action is accompanied by specifications for the EU C-ITS Security Credential Management System (EU CCMS), harmonised C-ITS services, and the development and implementation of C-ITS services. Of the aforementioned specifications, the EU CCMS specifications have already been published and are also an integral part of this study. The working programme states that ‘[c]ommon specifications could take the form of a new delegated act or an amendment to an existing delegated act’. In practice, this may lead to the start of the preparation of a new Delegated Regulation on the implementation of C-ITS as part of the working programme.

Finland’s national intent to promote the digitalisation and automation of transport sector has been described in key administrative publications, although they contain only a few references to the actual implementation of C-ITS. However, the development of C-ITS can be considered to be part of and one of the key actions for promoting the digitalisation of transport. From this perspective, it could be said that several potential entries that indicate support for the development of C-ITS have been made.

The only publication from Finland’s administrative branch that actually references C-ITS services is “Liikenteen automaation lainsäädäntö- ja avaintoimenpidesuunnitelma” (“Action plan on legislation and key measures of transport automation”, Miettinen et al. 2021). In this publication, C-ITS implementation is discussed from the perspective of information utilization and the information-sharing infrastructure required for road traffic automation. The document identifies the information transmitted by C-ITS messages as essential for promoting automated mobility.

The Government Programme of Prime Minister Petteri Orpo (Finnish Government 2023) contains a separate chapter on the renewal of transport services through digitalisation. In this context, the measures promoted by the Government include digitalisation and automation in the transport and logistics sector, the creation and utilisation of new business models, and the efficiency of the transport system.

The Government resolution on promoting transport automation (LVM/2021/137) also takes into account the connectivity and data exchange needs, and it contains a policy on significantly enhancing the exchange of transport-related data, paying particular attention to the development of mobile network technology and Finland's leading role in the field.

The Group Strategy of the administrative branch of the Ministry of Transport and Communications (Ministry of Transport and Communications 2024) sets several objectives for the use of digitalisation and data in the administrative branch. In particular, the objective of data-based transport services could be promoted through C-ITS development. One key driver for the development of C-ITS is improving road safety.

The Traffic Safety Strategy 2022–2026 (Rekola et al. 2022) also recognises technological developments as a path for increasing traffic safety. One of the measures of the strategy is to promote an operating model in which the data produced by vehicles and infrastructure can be utilised in generating a real-time and predictive situational picture of weather and road conditions. Such interconnections and data sharing between infrastructure and vehicles is expected to result in a number of road safety benefits. C-ITS represents a concrete way of achieving these goals.

The draft "Liikenne 12" ("Transport 12") plan for 2026–2037 for updating the national transport system plan (Finnish Government 2024), which was being circulated for comments at the time of this report, includes a separate chapter that focuses on the development of a digital operating environment for transport. As part of its focus areas, the plan places particular emphasis on the development of national operating models that support the production, sharing, and utilisation of information on the transport system in a cost-effective and value-generating manner. It also identifies the development of communications connections (comprehensive mobile networks) as a prerequisite for the digitalisation of transport.

The implementation of C-ITS services is one concrete method for advancing these upper-level strategic objectives. From the perspective of the C-ITS implementation, the documents highlight a strong link between the digitalisation of transport and communications connections, which can be considered to support an implementation model based specifically on a long-range communication solution.

The mapping of national perspectives on C-ITS also included an expert workshop that featured key national actors in the administrative sector, as well as representatives from Finnish municipalities. In Finland, public actors are largely responsible for the maintenance, development, and traffic information of road and street networks, so these actors also play a natural role in organising C-ITS services. The views expressed during the expert workshop reflected the participants' personal views, which may not necessarily align with the official positions of Finland's administrative actors and agencies. However, these participants play key roles in the C-ITS implementation in these organisations, so their views were a reasonably accurate reflection of Finland’s general intent on the topic.

Based on the results of the expert workshop, the understanding of the benefits brought by C-ITS services and the implementation timeline are partly unclear. This was particularly emphasised with long-range communication solutions. On the other hand, the participants expected regulatory changes to create a trust-based cooperation environment that will support the development of C-ITS services. They favoured a gradual deployment of C-ITS services, as this would enable the incremental development of operations and risk management. The participants strongly favoured an implementation model based on a long-range communication solution, despite the partly vague or inadequate regulatory framework, as it is seen as a cost-effective alternative to implementing the national C-ITS system. Cooperation with actors from other countries – and especially from other Nordic countries, with whom Finland has cooperated previously – was considered a very potential approach, as it enables the sharing of costs and expertise between different actors. This type of cooperation would also provide a broader pool of resources and a stronger foundation for service development. In addition, a co-creation model could provide Finnish actors with access to new markets and promote their competitiveness internationally. The participants also felt that the use of the National Access Point (NAP) in compiling and producing source data for C-ITS services would serve as a good operating model, as it promotes the quality assurance of source data and it is the most straightforward model from the perspective of C-ITS station operator-related responsibilities.

11 Proposal for a C-ITS implementation model in Finland

11.1 Main policies of the implementation proposal

The proposal to advance the readiness for the implementation of C-ITS services is based on the views of the working group and the results of the expert workshop organised for stakeholders. The working group's views are based on a literature review carried out during the work, external expert interviews, and the experts' own experiences with the relevant themes. The expert workshop was used to gather the views and expectations of key actors, as well as Finland's national intent for the implementation of C-ITS services. The main policies of the national C-ITS implementation proposal are listed below, and a more detailed breakdown of each policy is presented after this list.

- The implementation is based on a long-range communication solution.
- The implementation will be made gradually, but the process will begin immediately.
- A community-driven open source development model will be utilised where possible.
- The implementation takes into account the commercial strategies related to the deployment.
- The National Access Point (NAP) will play a key role in the national deployment of C-ITS services.
- The national C-ITS implementation will require the public sector's support.
- High-quality input data is critically important.
- To ensure privacy, the implementation will begin with I2V (Infra-to-Vehicle) messages, which do not contain any personal data.

Figure 18 illustrates the architecture and operating principle of the national C-ITS implementation proposed in this chapter. Items 2A, 2B, and 2C present alternative approaches. Items 5A and 5B are also alternative, but not mutually exclusive approaches.

1. Information on a road or street network event is produced in a digital format. This can be for any service; in this example, the information is roadwork related and produced by a contractor on a roadworks site. The information may be in a format defined by the contractor or in a known format developed for the transmission of traffic information, such as DATEX2.

2A. The information is transmitted from the contractor's systems to the central C-ITS station (operated by the municipality). This can be achieved by using the DATEX2 API or the central station operator's solution to convert the contractor's data to a suitable format.

2B. The information is transmitted from the contractor's systems to the national central C-ITS station. This can be achieved by using the DATEX2 API or the central station operator's solution to convert the contractor's data to a suitable format.

2C. The information is transmitted from the contractor’s systems to the NAP. This can be achieved by using the DATEX2 API or the NAP operator’s solution to convert the contractor’s data to a suitable format.

3. The NAP transmits the information to the national central C-ITS station. The data content can be converted to a format supported by the central C-ITS station, but the messages can only be signed by the central C-ITS station.

4. The central C-ITS station generates the C-ITS message. Based on the data content received, an ETSI standard-compliant C-ITS message is generated, to which the header fields required for IP-based data transfers are also added.

5A. The C-ITS message is transmitted between central stations according to the BI protocol. In this case, a BI protocol-compliant interface must be built between each connected central C-ITS station.

5B. The C-ITS message is transmitted between interchange servers according to the II protocol. In this case, there is no need to build a separate interface between each connected central C-ITS station. Instead, the interchange server ensures connectivity with other central stations.

6. The C-ITS message is forwarded to the end-user. The service provider operates its own central C-ITS station and transmits C-ITS messages to end-users.

The C-ITS implementation architecture presented in Figure 18 also demonstrates the boundaries of the EU CCMS, i.e. when C-ITS messages must be signed (area marked in blue). In practice, this provides a high degree of flexibility in, for example, how road operators produce their data and how service providers transmit messages to end-users. Although certain parts of the architecture in Figure 18 are not covered by the EU CCMS’s specifications, it does not remove the C-ITS station operator’s responsibilities for the confidentiality, integrity, or availability of the data used to generate C-ITS messages. Interchange servers are also exempt from this trust model, as they only transmit C-ITS messages instead of generating or signing them.

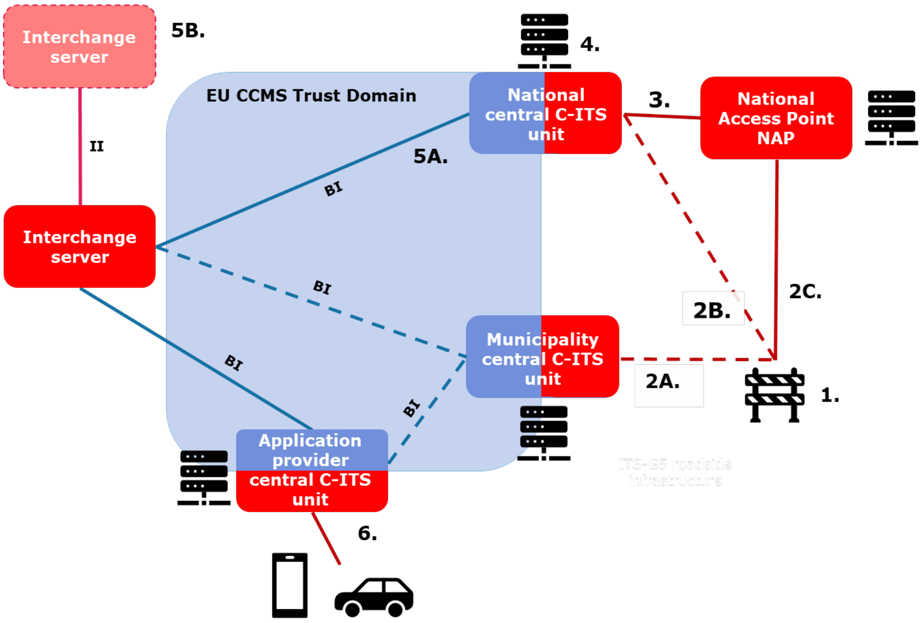

Interchange server
5B.
4.
II
EU CCMS Trust Domain
National central C-ITS unit
3.
National Access Point NAP
5A.
BI
Interchange server
BI
BI
2C.
2B.
Municipality central C-ITS unit
2A.
1.
BI
ITS-G5 roadside infrastructure
Application provider central C-ITS unit
6.

Figure 18. Illustrative diagram of the national C-ITS implementation architecture.

The implementation is based on a long-range communication solution

The research questions guiding this study have specifically focused on C-ITS implementations based on long-range communication solutions. Accordingly, key government publications and strategic documents emphasize the suitability of mobile network technologies for transport, supporting the preference for long-range data transmission. This can be seen as supporting, from the perspective of developing C-ITS systems, an implementation model based specifically on long-range communication solution. Mobile network connections play a crucial role in implementations relying on long-range communication, and the capabilities and development trends of these networks are examined in more detail in Chapter 9 of this study. Despite certain challenges, current mobile networks already provide a fairly comprehensive solution for the needs of C-ITS services. Furthermore, it can be assumed that the development of future network technologies and new features will support the deployment of C-ITS services based on long-range communication solutions. However, this study has not specifically assessed the capabilities of different communication technologies to implement individual C-ITS services (in accordance with the limitations set out in Section 1.2) nor the potential cost impacts of various technologies on implementation.

In practice, relying on long-range communication means that the implementation is based on data communication between central C-ITS stations located within an IP network and the use of mobile networks to connect roadside and street devices as well as end users. Additionally, this solution requires an interchange server to integrate the system into the European C-ITS ecosystem. During the initial stages of implementation, this interchange server may be located outside Finland, as connecting to it enhances the discoverability of C-ITS messages from individual central C-ITS stations in Finland.

In other words, the practical implementation process involves procuring or developing a central C-ITS station, deploying and operating it, implementing the station operator’s information security management system, deploying certificate services, and procuring or developing an interchange server along with its deployment and operation. More specific and detailed measures related to these steps are presented in Chapter 11.2, which focuses on the implementation and project organisation process.

The implementation will be made gradually, but the process will begin immediately

The aforementioned national C-ITS implementation and its long-range communication solution will require several procurements or development projects. Sufficient time should be allocated for the process from procurement preparation to implementation and maintenance, which is why it is recommended that the necessary steps be initiated without delay. However, the report includes sections that focus especially on the definitions related to the implementation of long-range communication, which are expected to become more specific as the work of the C-Roads Platform working groups progresses. For this reason, it is challenging to fully plan the national C-ITS system as a whole, and we therefore recommend promoting its development work gradually while actively participating in key definition and cooperation forums. A more detailed description of the implementation and its organisation is presented in Chapter 11.2.

The national implementation model should assess the possibilities of procuring the central C-ITS station and interchange server as a commercial solution, as a tailored, custom-developed solution, or as a community-driven open source solution. Each of these options presents its own strengths and challenges.

Commercial products generally include continuous development and product support due to market and regulatory requirements, as commercial operators have an interest in maintaining the compliance of their products. Competition between operators encourages product development and reduces costs. The procurement of a commercial solution also typically includes the other vital parts of a system's platform and operating services, such as server rooms, cloud services, telecommunications, information security, monitoring, maintenance, and user support services, in which case the client does not need to acquire these through separate means. Although commercial products are usually designed to meet the necessary general requirements, their deployment typically requires localisations and integrations that come with the deployment of an off-the-shelf solution. One example is the integration of data sources related to the operating environment. If the client is aware of their localisation and integration requirements during the tendering process, they can be included in the invitation to tender as requirements related to the product and its deployment.

Like all options, commercial solutions also include risks. One key risk is the lack of a versatile, evolving, and multi-option network of solution suppliers. A robust network is typically needed to ensure that there will be sufficient competition in the market, rapidly evolving solutions, and active innovations by companies keen to differentiate themselves from the rest – and all of these help keep prices down to reasonable levels. If this is not the case, the potential risks include those related to general cost levels and the slower development of products. This may lead to supplier dependency, which may then lead to increased costs if the solution cannot be easily put out to tender, for example due to interoperability problems or high replacement costs.

Of course, it is good to be aware of the fact that a custom-developed solution is not a risk-free option, even when compared to a procured solution. A key risk is the management of lifecycle costs, as this type of solution will require continuous development after the completion and implementation of the first version, which must be purchased as separate specialist work. In the case of extensive implementations, it may take a great deal of time for a specialist to take control of a solution, should there be a need to change software development partners or key individual developers. Changing a software development partner can sometimes be a very complex and expensive process. In addition to the continuous development of a customised solution, the platform, operation, and maintenance services for the solution must be procured separately, and they should be taken into account when comparing the cost levels of different solutions.

Switching between product-based solutions has been made easier in particular by the Europe-wide specifications and standards related to C-ITS back-end systems (central C-ITS stations and interchange servers), which ensure interoperability between solutions from different suppliers. When switching between product-based solutions, the new solution provider must be required to create the necessary integrations with national input data interfaces (the adaptation of a product-based solution to the national operating environment, i.e. localisation). This provides a good basis for commercial operators to develop products and solutions that can be deployed extensively in Europe.

The issue is also not unambiguous from the perspective of the security of supply, as large international actors may have better capabilities for ensuring the functioning and recovery of their systems in the event of disruptions. However, C-ITS messages are likely to play a minor role in critical infrastructure, especially in the early stages of their implementation, if the related services are allocated to an informative rather than a safety-critical or directive role (as discussed in Chapter 9.1).

The implementation of the C-ITS ecosystem should pay particular attention to scalability, i.e. allowing for the inclusion of more central stations at later stages. The gradual deployment process can be started with the implementation of the national central C-ITS station, which will be responsible for e.g. road network C-ITS services. However, according to the findings of this report, the C-ITS implementation process could also include situations where e.g. municipalities may be interested in introducing their own central C-ITS stations. A city-specific central C-ITS station is the right choice for cities that wish to offer more versatile C-ITS services, compared to what is possible with just the national C-ITS station (e.g. warning services for traffic congestions or approaching emergency vehicles). This type of situation is described in more detail in Chapter 6.5.

A community-driven open source development model will be utilised where possible

Based on the expert interviews, the study identified that commercial solutions are not yet fully mature in all respects, especially due to shortcomings in the definition of solutions based on long-range communication. For this reason, a procurement always involves a certain amount resource allocation and risk-taking. On the other hand, the study also identified that, as a result of Europe-wide standardisation related to C-ITS, all countries have very similar requirements for C-ITS stations and interchange servers. This feature also enables communal development between different countries, which could be implemented as a community-driven open source project, in accordance with the EU’s open source strategy.

A more detailed examination of community-driven open source activities was not included in this study, but its utilisation is described in Chapter 7 as part of the examination of the implementation options for the interchange server. The same development model is equally well suited to the development of the central C-ITS station. This study identified several benefits in the community-driven development of open source code, making it an attractive option. This option could be used to, for example, share development costs and competence. The development of an open source community can also guarantee a good level of development management and quality control processes. In addition, a solution made by several actors committed to the same implementation is likely to receive greater emphasis in the cooperation forums where C-ITS regulation is developed. The expert workshop also extensively highlighted the benefits of fostering an open source community. The challenges identified in this development model include the potentially demanding administrative work for establishing a community, such as creating a community governance model that is satisfactory to all countries, agreeing on costs, and determining a common target state and priorities for the development work.

The implementation takes into account the commercial strategies related to the deployment

The role of public administration in the implementation of these types of development projects should be examined. An essential characteristic of the Finnish national market is its limited number of customers. If Finland’s public administration decides to develop its own central C-ITS station solution as a separate development project (i.e. puts out a tender for a development team to implement the tailored solution) instead of acquiring it as a product-based solution from a commercial operator, Finland may not be able to foster more operators who offer commercial solutions.

The domestic market serves as an important reference for Finnish companies aiming to export their expertise. The digital services and platforms for transport sector companies are expected to generate export revenues that will support Finland’s economic growth and strengthen its pioneering role in the adoption of digitalisation and promotion of sustainable development. In 2024, a traffic data export cluster coordinated by Fintraffic was established to promote these efforts. The aim of the cluster is the extensive deployment of Finnish-developed traffic data services in Europe, thus opening up business opportunities for Finnish companies in the field. The cluster aims to enable larger export projects that could not be achieved by individual companies alone (Export cluster, n.d.). One of the early-stage joint innovations of the cluster’s companies is mobility services and data, so integrating the development of C-ITS into the cluster’s operations could help support both national C-ITS development efforts and the activities of companies in the sector. The national implementation model recommends that the development of product- and service-based C-ITS solutions by Finnish technology actors should be taken into account when considering different approaches.

The study also highlighted national commercial strategies related to open source communities. This approach emphasises the planning of an open source community in cooperation with the domestic private sector. A key part of the model is the creation of a strategy at the start of the development work to determine which parts of the final solution will be implemented by the open source community (e.g. key core technologies and platforms) and which parts will be left to the private sector (final commercialisation). These private sector characteristics can include, for example, the business critical features of the final solution, corporate innovations, and the usual commercial approach to open source solutions, i.e. providing product support for the final open source product. This type of approach allows public administration actors to strongly control the development of the solution and require the use of the open source code as part of its product-based procurements (technology requirement related to competitive tendering). This model would allow the companies in the sector to participate in the open source community, providing them with the opportunity to assist in the open source development and commercialise their own solutions based on the open source code. In an optimal situation, this model would also allow the public and private sector to be actively involved in the development of the solution, the private sector could create products and services based on the open source code, and the private sector would also gain national references as Finland’s public administration opted for its open source-based solutions rather than the open source solution itself (which was never designed to serve as the final solution in the first place).

The National Access Point (NAP) will play a key role in the national deployment of C-ITS services

One of the results of this study is that the NAP should be understood a central part of the national C-ITS ecosystem and its development. As a stand-alone system, it is not actually part of the C-ITS system defined by C-Roads Platform, and is therefore not subject to the same requirements. However, the NAP plays a broader role in the distribution of road transport-related information and is instrumental to the development of the ITS sector and the related systems, so it is worth investing in its development.

In many cases, the types of data that are transmitted to the National Access Point (NAP), such as real-time traffic data and traffic safety data, can be used to generate C-ITS messages. The central C-ITS stations can use the NAP to access real-time traffic system data, such as traffic sign data and the related impact areas, weather conditions, disruptions, or the locations of roadworks sites. This data can be used to generate related C-ITS messages that C-ITS service providers can convey to their end-users. End-users can be provided with informational and warning messages through C-ITS mobile applications developed by service providers, or the information can be transmitted directly to vehicles that are already equipped with an integrated vehicle C-ITS station.

From this perspective, the National Access Point (NAP) can be considered to serve the entire transport sector instead of just the C-ITS ecosystem, so its role is broad. The NAP is a national platform service for digital infrastructure, so individual actors do not need to invest in their own solutions to utilise traffic data. Each city has the right and opportunity to use the NAP to develop the service level of their respective transport systems. Simply put, the NAP provides a freely accessible infrastructure with widely available traffic data, and C-ITS is one concrete way of utilising this infrastructure. C-ITS can also adapt functions that, so far, have been implemented through national solutions – such as priority arrangements for emergency vehicles – and implement them via central C-ITS stations. This enables intelligent transport services to be technically implemented and managed from a single point.

The national C-ITS implementation will require the public sector’s support

The results of the study have mainly been targeted at public sector actors, while also taking into account the perspectives of commercial service providers and the rest of the private sector. The implementation of a functioning C-ITS system as a whole will require the involvement of commercial operators. However, public sector actors also play an important role in the C-ITS ecosystem, as they own and manage a large part of the transport infrastructure, such as road and street networks and traffic lights, which are essential for the functioning of C-ITS service implementations. This role is particularly emphasised in the construction of the required underlying digital infrastructure, which in this context refers to, for example, central C-ITS stations and an interchange server. Administrative roles, such as certificate management and the licensing of C-ITS stations, should also remain in the public sector.

The provision of end-user services cannot be unambiguously described as an activity of either the public or private sector, as both parties have their respective strengths in this context. Private sector services are characterised by their effective delivery in a competitive environment, where market mechanisms regulate supply and pricing. In this case, a competitive setting may improve the quality and cost-effectiveness of services, for example. In the current market situation, many of the parties providing end-user services for road users are private companies. On the other hand, the public sector may also be well placed to provide certain end-user services. For example, the Fintraffic Mobile application is used by numerous Finnish road users who wish to obtain traffic situation data. In any case, from the perspective of C-ITS development, commercial operators need certainty and a longer outlook for their investments. The public sector can provide these by investing in the development of the C-ITS system’s back-end infrastructure. Without the public sector’s investments, the time span of the C-ITS implementation will become longer and even uncertain.

High-quality input data is critically important

The significance of high-quality input data is emphasised in the C-ITS implementation based on long-range communication. This is because the operators of central C-ITS stations are responsible for the reliability of the input data used to generate C-ITS messages, in accordance with the C-ITS Security Policy document (see Chapter 4.2, which discusses the operational management of C-ITS stations). In other words, ensuring the timeliness and quality of data is a key issue that must be resolved to ensure that, for example, the data collected to the NAP, and the C-ITS messages generated on the basis of this data, could be considered a valid implementation model for C-ITS services.

Quality specifications are being developed in different forums. For example, the RTTI Task Force, which works closely with the NAPCORE project and consists of road and other operators in the EU, has initiated the development of a star rating-based quality specification for RTTI-related data (1–5 stars, like in EURO NCAP collision tests). The Task Force’s work is based on a proposal made by road traffic information service providers who belong to the Traveller Information Services Association (TISA). At the time of this study, the RTTI Task Force was still working on the matter, but it has not published any official quality criteria. The Data for Road Safety ecosystem (DfRS ecosystem), which distributes road safety data from the automotive industry, traffic information service producers, and road operators, has developed a quality specification for SRTI data. This specification focuses on the quality level of data publications in the ecosystem, where the participating actors themselves can rate the quality level of each message as either A or B, with a significant difference in accuracy between these two quality levels. This study recommends striving for an A level of quality, and it is even questionable whether a B-class quality level is sufficient for generating C-ITS messages in central C-ITS stations. C-Roads Platform has not published a separate document that describes the quality specification of C-ITS services, but its Service and Use Case Definitions provide some indication of what the data content should be.

Fintraffic is involved in both of the forums referenced above. The main recommendation of this study is that the active work in these forums should continue, and that it would also be worth assessing whether these quality attributes are sufficient for the activities of central C-ITS station operators (to meet the requirements of the C-ITS Security Policy), if this data were used to generate C-ITS messages.

To ensure privacy, the implementation will begin with I2V messages, which do not contain any personal data

According to the C-Roads Platform specification, I2V (Infra-to-Vehicle) C-ITS messages do not contain personal data on the basis of their data content (payload). These include warning messages related to road works and road conditions delivered from road operators to vehicles. In addition to the data content itself, C-ITS messages contain the sender's public PKI certificate, in accordance with the EU CCMS. This certificate ensures the integrity of the data, but it also provides a technical opportunity for identifying the sender through the certificate. However, tracking based on the public certificate (e.g., of a vehicle) is limited by privacy-enhancing measures, such as frequently changing certificates and short data retention periods. The technical possibility of identifying the sender is created by combining indirect and multiple sources of information.

In IP-based long-range communication solutions, C-ITS messages are encrypted using the TLS protocol. Thus, the TLS protocol also serves as a risk management tool for the PKI certificate within the message envelope. The IP address itself is personal data and is necessary for the delivery of the message. This data is accumulated by message intermediaries, such as telecommunications operators. Telecommunications operators are subject to various regulations, such as the Act on Electronic Communications Services, and the related transmission data may only be disclosed to those parties that have the right to process this data. Telecommunications operators can only share anonymised information about their customers.

On these grounds, and to ensure privacy protection in C-ITS implementation, it can be assumed that I2V-type C-ITS messages in long-range communication solutions do not constitute personal data and therefore do not require a legal basis for processing. This assumption could serve as a practical starting point for establishing C-ITS systems. However, a data protection statement describing the processing (as in the example of the DfRS ecosystem) should be drawn up to describe the data processing procedure.

However, if the formation of a personal data file is considered necessary (and every party collecting and sending data must assess this on a case-by-case basis), then in the absence of a C-ITS Directive, the *public interest* could be used as the basis for processing I2V-type C-ITS messages. The public interest requires a legal basis that determines the necessity and category of such processing. This legal basis must be sufficiently precise and detailed to ensure that the processing is justified. The most likely options are the Road Traffic Act (729/2018), the Act on the Finnish Transport Infrastructure Agency (862/2009), or the Act on Transport Services (320/2017). For the trans-European C-ITS implementation, it is assumed that EU-level regulation will provide the applicable processing grounds, for example in the context of the Delegated Regulation on C-ITS.

11.2 Deployment and organisation

This chapter describes in more concrete terms how the proposed national implementation model for the architecture of C-ITS services, which was presented in the previous chapter (11.1), will be deployed. This chapter also describes how actors in the administrative sector should be organised to promote the implementation process. The proposed organisational model is the consultant's suggestion, based on the division of roles between authorities proposed by Kotilainen et al. (2023). As such, the proposed organisational model does not represent the administrative sector's actual plan for organising the implementation process.

Implementation of the central C-ITS station

The recommended implementation path for the deployment of the central C-ITS station is presented in more detail in Figure 19, which relies on the long-range communication solution based on the reasoning provided in the previous chapter. In this case, the relevant section is contained in the upper half of the figure. When a C-ITS system is implemented using a long-range communication solution, it is based on data transfers between central C-ITS stations. The central station is a software-based solution, and the station operator can either create their own station (by developing it themselves or through an open source co-creation model with other actors), or procure a commercial product.

As has already been stated in this report, the technical development, standardisation, and definition of the European C-ITS system has, from the outset, been very strongly based on the use of a short-range communication solution. Despite the C-Roads Platform working groups' efforts to define a long-range communication solution, the model still contains unresolved issues, such as the lack of protection profiles for central stations and the requirements for using HSMs in data centre environments. As a consequence of these deficiencies, no commercially created central C-ITS stations complying with the requirements of the EU C-ITS system (especially L2) were fully ready at the time of writing this report. In connection with this study, Chapter 5.2 identifies and presents commercial operators whose solutions on the market are widely used regionally, but do not fully correspond to the C-Roads Platform specifications (e.g. in the signing of messages). However, commercial operators have the capacity and business interest to adjust their products to comply with the specifications. Therefore, it is recommended that authorities clarify these specifications to promote the development of compliant commercial products.

For the aforementioned reasons, no single implementation model can be unambiguously recommended – instead, the feasibility of different alternatives should be examined once the implementation of the central C-ITS station becomes relevant. Procuring the central C-ITS station as a commercial product requires the clarification of requirements according to C-Roads Platform specifications. This clarification would ensure the consistency of solutions offered in the market. The preconditions for implementing the central C-ITS station as a joint development process hinges on finding other actors committed to the development process and forming a jointly functioning administrative and business framework.

The rationales for purchasing a commercial, off-the-shelf product should also be examined critically. The procurement and deployment of an off-the-shelf product typically requires tailored solutions related to the localisation and integration of the product during its deployment. However, caution should be exercised during the tailoring process, as any excessive customisations may make the solution difficult to replace, thus leading to a so-called vendor lock-in situation. Therefore, where possible, it is advisable to keep the product in line with the specifications and standards in terms of its core features. It should also be noted that, as a rule, any changes to an existing product can only be implemented by its owner, meaning that the updates and customisations cannot be put out to tender. In critical systems, the procurement of product-based closed solutions may include special terms and conditions for the management of intellectual property rights related to the source code. These so-called escrow clauses protect the buyer of closed software in situations where the software supplier goes bankrupt or is otherwise unable to fulfil its maintenance and support obligations. The clauses define the terms and conditions under which the software's source code and the related documentation are handed over to the buyer.

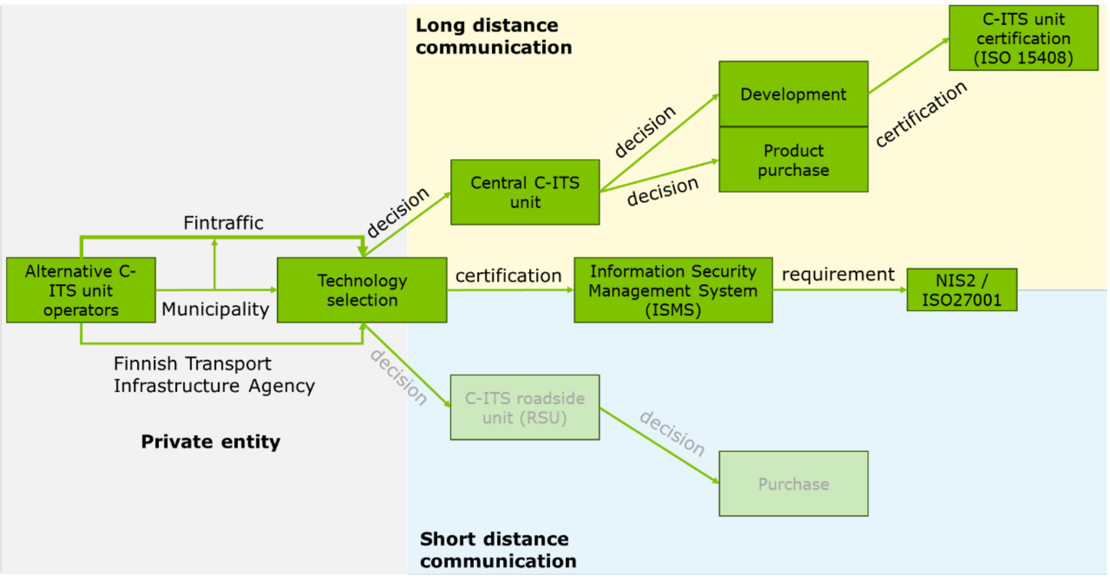

Long distance communication
C-ITS unit certification (ISO 15408)
Development
Product purchase
certification
decision
decision
Central C-ITS unit
decision
Fintraffic
Alternative C-ITS unit operators
Municipality
Technology selection
certification
Information Security Management System (ISMS)
requirement
NIS2 / ISO27001
Finnish Transport Infrastructure Agency
decision
C-ITS roadside unit (RSU)
decision
Purchase
Private entity
Short distance communication

Figure 19. Implementation and operation of the central C-ITS station (highlighted: recommended path forward and alternatives to be examined in more detail).

Figure 19 also includes an ISMS, and it can be noted that, regardless of the type of C-ITS station, the station operator must have a certified ISMS in place. This typically means an ISO 27001-compliant management system, but parties operating an essential transport service may also apply the requirements of the NIS2 Cybersecurity Directive to their information security management. An ISMS is an internal development project of an organisation acting as a station operator, and it is used to develop the organisation's information security management and the related operational processes and tools. The system must take into account and be consistent with the C-ITS Security Policy. At the time of writing this report, Fintraffic, the relevant entity in relation to the role of the national central C-ITS station operator, was developing an information security management system.

Deployment of certificate services

As described in Chapter 5.4 of this study, the C-ITS station operator must make a decision on which EU CCMS certificate service provider it will work with to register and manage its C-ITS stations. The recommendation of the working group on the introduction of certificate services is presented in Figure 20 below. This recommendation is based on the utilisation of commercial solutions. Other alternatives include using the root certificate offered by the EU or developing a custom solution. Based on the results of this study, it can be concluded that the free EU root certificate service maintained by Atos is mainly intended for pilot projects, and it was not originally intended to be used in large-scale, finalised L2 production environments. It is also unclear whether the maintenance of the EU root certificate service will continue after the end of its current contract period (end of 2026) as, in the specifications under the new ITS Directive, the European Commission has no official role or responsibility in the provision of the service in question. For this reason, basing the national certificate service on the free certificate service maintained by Atos is not recommended, although it can still be used for piloting purposes. Developing a custom root certificate, on the other hand, would require a significant amount of effort, expertise in the topic, and resources for both its development and maintenance, so it cannot be recommended as an implementation model without reservation.

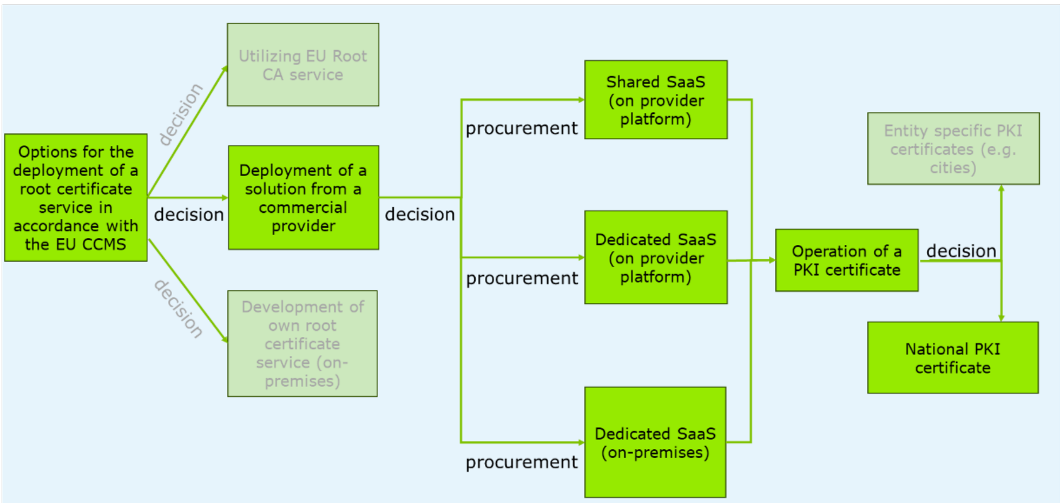

Options for the deployment of a root certificate service in accordance with the EU CCMS
decision
Utilizing EU Root CA service
decision
Deployment of a solution from a commercial provider
decision
Development of own root certificate service (on-premises)
decision
procurement
Shared SaaS (on provider platform)
procurement
Dedicated SaaS (on provider platform)
procurement
Dedicated SaaS (on-premises)
Operation of a PKI certificate
decision
Entity specific PKI certificates (e.g. cities)
National PKI certificate

Figure 20. Procurement and operation of certificate services (highlighted: recommended path forward and alternatives to be examined in more detail).

Commercial operators have several solutions for the implementation of certificate services that meet the requirements of the EU CCMS. In small-scale or one-off environments, it is easiest to use the shared certificate offered by root certificate service providers. This approach does not require any separate approvals or audits from the certification policy authority for the implementation of the service, as the operating environment used to deliver the service already meets these requirements. Based on discussions with service providers, this model functions quite well even in larger-scale implementation environments. Our recommendation is to start with this model as a starting point for the national implementation. As these activities expand or potential risks are identified, the operations can be developed into solutions that better meet customer needs, which are presented in the following sections.

If it is determined that a customer-specific certificate service would be a necessary choice, a SaaS-based service model can still be used, in which the service provider establishes a separate service environment for the customer. In this case, the new certificate service is registered in the EU CCMS, and it must undergo all approval procedures that apply to certificate service providers. The service provider will be responsible for the necessary approvals, but this will increase the administrative work and costs related to the environment. This model has been used to implement national (e.g. Czech Republic), city-specific (Hamburg), and organisation-specific (e.g. Autobahn and ASFINAG) certificate services. If risks related to national or organisational security are identified in the SaaS-based implementation of the certificate service, the root certificate service can also be established in the country's or organisation's internal data centre environment (local implementation). However, this approach is likely to involve more costs and requires establishing or procuring a high-security data centre environment and assuming a larger role in the environment's management and the related, EU CCMS-mandated continuous approval procedures. In this case, the physical quality level of the service environment is also subject to specific requirements, and the responsibility for managing this environment is borne primarily by the customer. The study identified no management or cybersecurity needs that would justify these options, at least in the early stages of the C-ITS implementation.

From the perspective of the operational management of certificate services, either operator-specific PKI certificates (e.g. city-specific certificates) or a national PKI certificate can be used. For the national C-ITS implementation, it is recommend to primarily rely on a national PKI certificate. The benefits of the proposed model identified in the study are related its simpler management process. A national certification service provider provides better control over the large-scale and long-term registration of C-ITS stations compared to a model where national C-ITS station operators independently select an operator-specific PKI certificate provider. The certificate service provider acts in partnership with the national authorities, and it applies its expertise in matters related to the registration of C-ITS stations. These actors are well-versed in the requirements and certification processes of the EU CCMS and are better equipped to define the necessary national registration policies. The aforementioned benefits are emphasised in situations where a single national authority, such as a competent authority, coordinates service-specific authorisations granted to C-ITS stations. When granting service-specific authorisations, it can be ensured that the applicant has or is granted access to the national root certificate service. The applicant can then be guided to register the new C-ITS stations in this service. This benefit is clearly evident in the introduction of C-ITS stations specifically for governmental use. The process for applying for the authorisation to use a station from the competent authority can be combined with the procurement of certificates from the national centralised service. The strengths of the alternative, actor-specific model are related to larger actors who want to develop the use of certificates and tailor their certificate management together with service providers. Examples of these include operators in the automotive industry and parties operating and managing large traffic environments.

Implementation of the interchange server

The requirements related to the interchange server are discussed in Chapter 7. This chapter also examined the different implementation options for the solution. The identified alternatives were a completely independent implementation of the solution, an independent implementation with the help of open source code, the community-driven development of open source code, or product procurement.

When selecting a development option, particular attention should be paid to the existing requirements related to the system under development. If the solution needs to be strongly tailored to specific needs, this favours the selection of a tailored implementation. On the other hand, a product-based procurement is the better option if the product is to be strongly defined on the basis of industry standards or regulation. In such situations, the market also usually generates more supply when there is greater demand for the same type of product. As such, the process for implementing the interchange server is very similar to the implementation of the central C-ITS station.

C-Roads Platform has issued several specific requirements related to the features of interchange servers. Their key functions and interfaces are defined in the C-ITS IP Based Interface Profile (2024). This background also provides a good basis for considering the procurement of product-based solution (provided that the necessary products emerge in the European market).

The use of open source code is also a credible solution. This line of implementation contains two options. One option is to use existing open source code in a tailored development project. The biggest benefit of this model is that it can accelerate the development process, since the open source code provides a good basis for development. On the other hand, using a significant amount of pre-existing code as the basis for a tailored solution also contains risks. The key challenges are the high-quality utilisation of the code in question (the code base may not be familiar to the developers) and challenging troubleshooting if the development work runs into any issues.

Another option is the community-driven open source development. This model includes joining or establishing an open source community (e.g. the Nordic community), which implements common guidelines for the development of the solution, agrees on funding models, and creates an administrative basis for the work. This model provides several benefits, such as sharing the financial risk, i.e. “doing more with the same money”, and potentially accelerating the development work when more resources are available. However, its risks include the significant amount of effort required to set up a community and possible disagreements on the direction of the solution’s development and the prioritisation of its development paths.

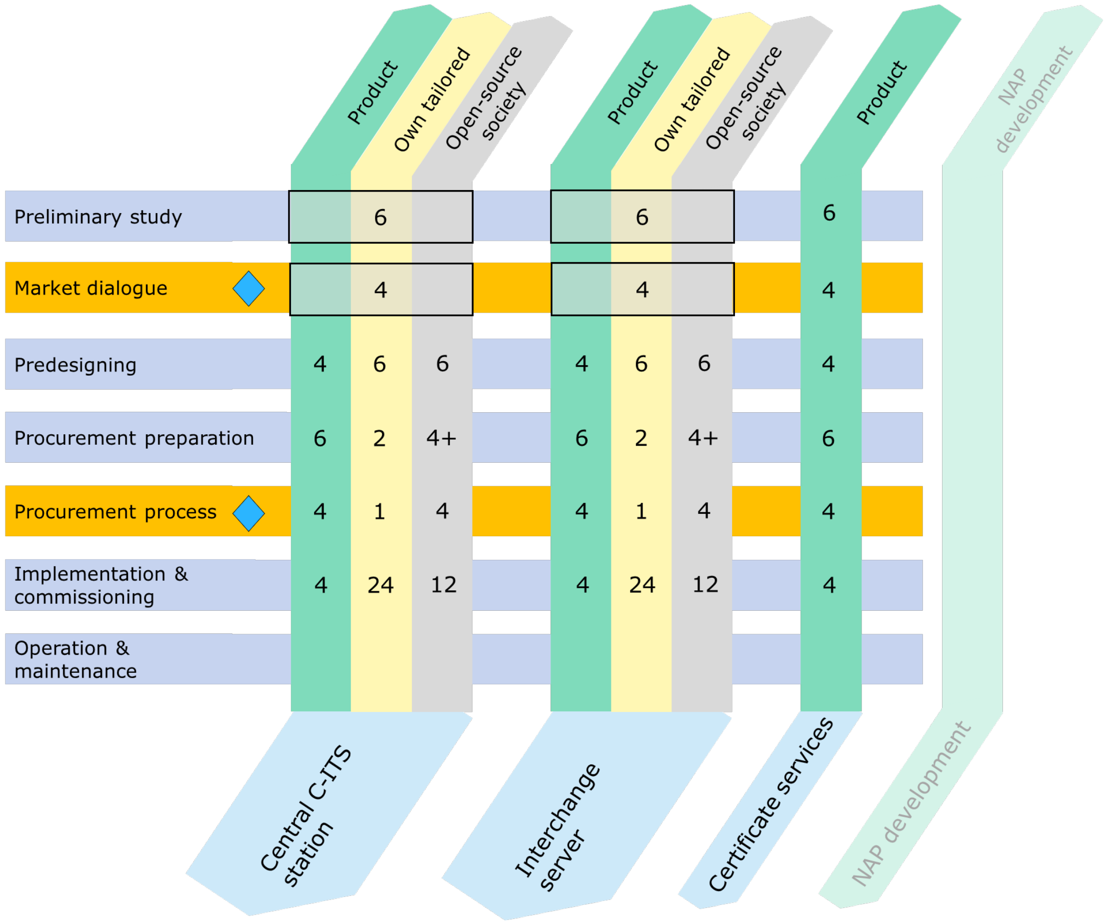
In general terms, when it comes to the development of the interchange server, it is not the most urgent task for the development of the national C-ITS system. The national C-ITS system can be launched with the help of, for example, one central C-ITS station and the services provided to end-users through mobile applications. As the system develops and more national, city-specific, or private central C-ITS stations are launched, and the need for cross-border connections increases, the interchange server will play a key role in connecting all of these elements. In the early stages of its operation, the central C-ITS station in Finland could also be connected to an interchange server located in another EU country. As it is assumed that, in the early stages, only one central C-ITS station will be operational in Finland, the findability of messages could likely be significantly improved in an alternative approach where the Finnish central C-ITS station is connected to an interchange server in a neighbouring area.

There are many options for implementing the interchange server, which is why it is a good idea to start planning its implementation immediately. This should include negotiations with potential co-development partners (willingness and similar intent) and investigations of existing open code alternatives (cf. Norway's open solution). At the same time, the parties should also investigate commercial solutions, and this approach could also be strengthened through national market dialogue and other similar measures.

Organisation

The promotion and development of C-ITS has generally been an administrative problem in the sense that the related responsibilities have not been clearly allocated or assigned. C-ITS has mainly been promoted through individual studies and small-scale experiments. To address these challenges and implement the measures outlined above, we recommend setting up a C-ITS Development and Deployment Coordination Group. The Coordination Group's concrete tasks for promoting the stages of the C-ITS implementation process are presented in Figure 21. The development of the National Access Point (NAP) has been taken into account as one of the actions related to the work of the Coordination Group, but it has been differentiated from other developments, as the role of the NAP is broader than that of C-ITS. The key objective of the Coordination Group is to promote the C-ITS implementation in a comprehensive and long-term manner, instead of a series of one-off projects and reports. The Coordination Group's work also involves an impact assessment of C-ITS services and implementation.

The roles of the authorities in the C-ITS implementation have been examined in a previous report published by Traficom (Kotilainen et al. 2023), and according to the role allocation proposed in the report, the role of the C-ITS competent authority and the service-specific authorisation issuer has been proposed to Traficom, in which case it is natural that Traficom would also be responsible for procuring certificate services. Both of the above are newly proposed roles. In the same report, Fintraffic was proposed for the role of the operator of the national central C-ITS station, so it is natural that the same organisation would also be responsible for the procurement or development of the central C-ITS station. The role of the central station operator is also new. In the same vein, the obvious choice would be to have the party responsible for the central C-ITS station also be responsible for the development or procurement of the interchange server. Fintraffic currently operates the National Access Point (NAP) on behalf of the Finnish Transport Infrastructure Agency, so it would be advantageous to share the responsibility for the development of the NAP among these actors, for example. The other important organisations for the implementation process include the Finnish Transport Infrastructure Agency and Finnish municipalities, as they play a key role in the development, maintenance, and data management of Finland's road and street network. The aforementioned organisations form the core of the C-ITS Development and Deployment Coordination Group. Any external assistance to coordinate the activities of such a group may also be justified.



	Central C-ITS station			Interchange server			Certificate services	NAP development
	Product	Own tailored	Open-source society	Product	Own tailored	Open-source society	Product	NAP development
Preliminary study		6			6		6	
Market dialogue ◆		4			4		4	
Predesigning	4	6	6	4	6	6	4	
Procurement preparation	6	2	4+	6	2	4+	6	
Procurement process ◆	4	1	4	4	1	4	4	
Implementation & commissioning	4	24	12	4	24	12	4	
Operation & maintenance								

Figure 21. Concrete activities of the C-ITS Development and Deployment Coordination Group.

Initially, the Coordination Group’s operating period could be set for a fixed term, in which case its task would be to proceed with the actions described in Figure 21 up to the market dialogue or competitive tendering phase.

The numbers shown in the figure refer to the number of months that each phase is estimated to take. The *preliminary study phase* for the different implementation options should be as neutral as possible. The status of available commercial implementations should be investigated through market surveys or dialogue. The prerequisites for custom development and co-development should be examined, for example, by assessing the available open source software and components and by surveying potential co-development partners.

Market dialogue is the first natural decision point at which a decision can be made on whether the C-ITS implementation should proceed, based on the results of the preliminary studies. If it is decided to proceed with the implementation, the *pre-design* of the selected implementation model and the *preparation of the procurement* should be initiated. The pre-design phase will presumably take less time in a product-based solution, as the properties and functionalities of the existing product set specific boundaries for the work. In the preparation phase of the procurement, however, more detailed specifications must be made on the product-based solution, or in the case of the co-development model, the participants must agree on several issues, such as administrative matters, guidelines for the development work, and the commercial strategy. The goal of both the pre-design and procurement preparation phase is to make the procurement process a reality.

The *procurement process* is another natural decision-making point for finding a supplier on the market that meets the minimum requirements and offers the most economically advantageous solution in terms of its price-to-quality ratio. If the process leads to a successful procurement, the Coordination Group can proceed to the *implementation and commissioning* phase. As can be seen in Figure 21, although the development work for a custom solution is easy and quick to start, for example through a framework agreement, the *implementation and commissioning* phase is likely to take considerably more time than the product-based approach. At this phase, the co-development model can be accelerated by, for example, the progress made by one's partner countries in the development process. After the solution has been successfully implemented, the Coordination Group can proceed to the *operation and maintenance* phase. However, even in this situation, the Coordination Group could still continue its work, as its assistance may be needed in the deployment of new C-ITS services or, for example, municipality-specific central C-ITS stations. The work should also involve actual C-ITS service providers, to promote mutual dialogue. While the process for implementing the central C-ITS station and the interchange server are similar, when it comes to the deployment of certificate services, the market situation for commercially available products is stronger and supports the procurement of the service from a commercial operator.

It should also be noted that the *implementation and commissioning* phase presented in the figure may, in reality, be divided into several phases, the first of which could be, for example, a more limited national implementation and starting with a 'minimum viable product'. Over the next phases, the aim could be to gradually expand the available functionalities by connecting the central C-ITS station to the trans-European network of interchange servers, thus enabling the central C-ITS station to share messages across Europe. The services implemented in the early phases should also be examined from the perspective of privacy protection. As long as there are no EU-level grounds for processing and established case law, the safest option is to focus on services that do not contain personal data. These include I2V (Infrastructure-to-Vehicle) C-ITS services (e.g. warning services related to road works or road conditions). From the perspective of privacy protection, Chapter 8.4 discusses the implementation of two Day 1 C-ITS services in more detail. However, this work does not include a more comprehensive service-specific examination of the deployment of the national C-ITS implementation. According to the results of this study, good and effective practices can help to compensate for shortcomings in legislation related to the protection of privacy. Cooperation can help clarify the responsibilities and operating models necessary for the safe and efficient implementation of C-ITS services. The establishment of the proposed C-ITS Development and Deployment Coordination Group is intended to contribute to this need.

The implementation process should also take into account the recommendations of the C-ITS security and certification policies for C-ITS station operators, which advise deploying C-ITS stations over several steps. This refers to the EU CCMS, which includes operating models for levels L0-L2, as described in more detail in Chapter 4.2.4. In short, the differences between these levels are that Level 2 corresponds to production use, Level 1 is intended for temporary production use and creating the preconditions for advancing to Level 2, and Level 0 is intended for piloting. The early stage technological development work can be carried out at Level 0. The process can then advance through the levels as the compliance and organisational aspects of the C-ITS stations are developed. Of course, it should be noted that the permanent production of the actual production services cannot be started until the activities reach Level 2. Such a step-by-step approach is not mandatory, but it should be considered nonetheless.

The Coordination Group should also actively participate in key forums and closely monitor the development of solutions based on long-range communication. The key forums identified in the previous chapter include the various C-Roads Platform working groups referenced in connection with the quality specifications (e.g. the Hybrid Communication working group), the Data for Road Safety ecosystem, and the RTTI Task Force consisting of road and traffic management operators in the EU. As the definition and development of the national C-ITS ecosystem progresses, the concrete proposals for implementation models can also be brought to these forums, thus ensuring the interoperability of the national implementation with the trans-European regulatory framework.

Risks related to the promotion of different measures

The risks of the measures related to the promotion of the national C-ITS implementation can be examined by classifying the measures into low-, medium- and high-level risks, in accordance with Table 19. In this context, the risks in the table refer to benefit-cost risks, i.e. how certain it is that the money and resources invested in the C-ITS implementation will produce socio-economic benefits. In other words, the risk category in the table depends on how much the measure is tailored to a specific C-ITS implementation model or what kinds of cost impacts it entails. As presented in the limitations of the study (Chapter 1.2), no actual assessment of the impacts of C-ITS services has been carried out in this work. Instead, the table aims to illustrate issues that should be addressed in the national implementation model.

Table 19. Risk classification of measures

Measure	Risk class	Description
Certificate service procurement	Medium	The certificate service must be procured in every C-ITS implementation option, regardless of the types of C-ITS stations used to implement the services. This reduces the risks related to procuring the certificate services. The risk is that if C-ITS services are not implemented, the certificate services would be unnecessary. This underlines that the implementation of all C-ITS components should proceed simultaneously.
C-ITS central station implementation	High	The risks associated with the implementation of the central C-ITS station and the interchange server are high, as several alternative approaches can be used for these two entities (commercial procurement, custom development/tailored implementation or open source-based co-development). The investments and the need for own resources vary depending on the implementation model, but are significant in each option. This risk can be managed through a gradual progress and implementation approach, in which case large investments are not made at once, but as the development work progresses and knowledge accumulates.
Interchange server implementation	High	
National Access Point development	Low	The large-scale collection of SRTI and RTTI data to the NAP and the development of a NAP to serve the generation of C-ITS messages have been identified as a low-risk measure. There is an obligation under the EU directive to collect data types, so these measures must be promoted in any case. At its simplest, the generation of C-ITS messages with the NAP only requires an interface development.

Although the promotion of the C-ITS service implementation architecture is subject to the risks presented in Table 19, it should be noted that not taking the measures related to the C-ITS implementation is not a completely risk-free option either. If the national C-ITS implementation is not promoted, Finland will have less influence in key forums, as its proposals will not be based on proven implementation models. There is also the risk that definitions and requirements that are contrary to Finland’s interests will be included in key trans-European documents guiding C-ITS development. A reactive role in the development of C-ITS would delay the national deployment of services, which would also delay the expected positive impacts of C-ITS services on the safety, emissions, and efficiency of the transport system. As has been demonstrated in this chapter, the time span from the start of the more detailed preliminary study on the implementation of C-ITS sub-systems to the operation and maintenance phase is likely to be several years.

12 Evaluation of results

This report presented a proposal for promoting the capabilities for deploying C-ITS services, taking into account the implementation and operation of the central C-ITS station in accordance with the EU's C-ITS security and certificate policies, the implementation of the EU CCMS, and the requirements for the interchange server and its deployment in Finland. The proposal also took privacy perspectives into account as part of the efforts to promote the capabilities of deploying C-ITS services in Finland. This chapter assesses the reliability of the work's results, as well as the related limitations and uncertainties.

The reliability of the results is generally influenced by the maturity of C-ITS technology, i.e. the incompleteness of the specifications and definitions for C-ITS services, and the limited experience in their application. As a whole, only a limited number of service implementations have been made in accordance with the C-Roads Platform and the EU's C-ITS security and certification policies. During the study, no existing implementations based on long-range communication solutions that met the criteria for EU CCMS-compliant Level 2 (production use) solutions were identified. In implementations based on long-range communication, the lack of protection profiles for central C-ITS stations and the requirements for the use of HSMs in data centre environments are examples of key issues to be defined.

The legislation on C-ITS services is also partly flawed – for example, the grounds for processing personal data in C-ITS services are not unambiguously defined. In relation to the legislative framework, Finland has a limited amount of capacity for making decisions, as many of the issues are within the competence of the EU, and it is not necessarily worthwhile to draft national legislation before EU-level policies, in order to ensure the interoperability of Finland's solutions across Europe. Therefore, the future development of regulation concerning these services is somewhat uncertain, as the development of EU-level regulation is difficult to predict. As an important follow-up measure, the report proposes influencing different regulatory frameworks through key working groups.

The significance of the study's results is increased by their novelty value, as only a limited amount of experiences has been gathered on applying the specifications related to C-ITS (incl. EU CCMS and C-Roads Platform profile specifications). The novelty value and significance of the results in the planning of the implementation and deployment of C-ITS services are also increased by the fact that there are no known service implementations based on a long-range communication solution that meet the necessary L2 requirements. The transition from piloting to existing production phase services is a topical theme in the development of C-ITS, and the results of this report particularly support this development.

The outcome of this study is a proposal for a national implementation model for C-ITS. The key research question was to identify whether the existing specifications contained any obstacles to the introduction of C-ITS services in Finland. No such obstacles that could completely prevent the implementation were identified during the work. However, the implementation process may to some extent be hampered by the requirements concerning the introduction of an ISMS that apply to station operators. The implementation of a certified ISMS in accordance with ISO 27001 is a significant cost factor for operators that wish to deploy new C-ITS stations. According to the estimates presented in the report, the lower limit for deployment costs is likely to be some tens of thousands of euros, with annual direct costs and indirect cost impacts going even higher. This may completely exclude the smallest operators from operating C-ITS stations (e.g. public transport operators, towing service providers, and smaller municipalities, as well as smaller software vendors), or, in the case of larger operators, the deployment costs may outweigh the expected benefits. This applies in particular to operators that fall below the size limits defined in the NIS Directives or that do not fall within the scope of the NIS Directives' other obligations, but are indirectly subject to the requirements, for example as a result of competitive tendering. As a follow-up question, it should be considered whether an alternative based on the NIS1 and NIS2 Directives could offer a more cost-effective pathway or ready-made national guidance to these actors, and which actors could potentially be covered by this option.

Although no actual obstacles to the deployment of the C-ITS system were identified, no unambiguous proposal could be given for the implementation model of the central station or interchange server, as this requires a more detailed preliminary study and market consultation to clarify the presented alternatives. The results of the report were also unable to unambiguously indicate whether the C-ITS implementation should be promoted, as the socio-economic benefits of the implementation have not been assessed. However, the report presents an implementation plan related to the possible deployment of the system providing C-ITS services and recommends that such an assessment be prepared as part of it. The report provides a good foundation and starting point for systematically continuing the promotion of C-ITS and its introduction in Finland.

13 References

Act on Electronic Communications Services 917/2014. Available at: https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#O6L17P138 (Accessed: 20 February 2025).

Almaviva interview, 2024, Teams, 21 October 2024, Subject: ”The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of C-ITS central units, the similar progress in Italy”.

Article 29 Data Protection Working Party (2017) Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) - wp252. Available at: https://ec.europa.eu/newsroom/article29/items/610171/en (Accessed: 20 February 2025).

Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., Schubert, T., 2021, “The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy”, Final Study Report, May 2021, European Commission.

CAR 2 CAR Communication Consortium, 2019, C-ITS: Cooperative Intelligent Transport Systems and Services. Website. Available at: https://www.car-2-car.org/about-c-its#c1001 (Accessed: 18 February 2025).

CCAM Partnership, 2023, Strategic Research and Innovation Agenda (SRIA). Available at: https://www.ccam.eu/wp-content/uploads/2023/11/CCAM-SRIA-Update-2023.pdf (Accessed 12 February 2025).

C-ITS Certificate Policy, 2024, "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) - Release 3.0 – May 2024", Ispra: European Commission, JRC137554. Available at: https://cpoc.jrc.ec.europa.eu/data/documents/E01941_C-ITS_Certificate_Policy_Release_3_0_FINAL.pdf

C-ITS IP Based Interface Profile, 2024, Version 2.1.0, C-Roads Platform, Working Group 2 Technical Aspects, Taskforce 4 Hybrid Communication, C-ROADS.

C-ITS Security & Governance, 2023, Version 2.0.7, C-Roads Platform, Working Group 2 Technical Aspects, Taskforce 1, 9 March 2023, C-ROADS.

C-ITS Security Policy, 2023, "Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) - Release 3.0 – September 2023", Ispra: European Commission, JRC133795. Available at: https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0._20230916.pdf

COSS ry interview, 2024, Teams, 25 September 2024, Subject: Use of open-source communities in public-sector software projects, 25 September 2024.

CPOC Protocol, 2024, “C-ITS Point of Contact (CPOC) Protocol in the EU C-ITS Security Credential Management System (EU CCMS) – Release 3.1 – June 2024”. Ispra: European Commission, JRC136507. Available at: https://cpoc.jrc.ec.europa.eu/data/documents/E01941_CPOC_Protocol_Release-3.1_20240627.pdf

C-Roads C-ITS Message Profiles, 2023: C-ROADS Platform Working Group 2 Technical Aspects Taskforce 3 Infrastructure Communication, 14 December 2023.

C-Roads C-ITS Service and Use Case Definitions, 2024, Version 2.1.0, C-Roads Platform, Working Group 2 Technical Aspects.

C-Roads webinar, 2024, Webinar: From Vision to Reality – Operational C-ITS Services, On June 26, 2024. URL: https://www.c-roads.eu/platform/about/news/News/entry/show/webinar-from-vision-to-reality-operational-c-its-services.html

C-Roads WG2 Deployment Documentation, 2024, Introduction to the C-Roads WG2 Deployment Documentation and Requirements, Version 2.1.0, C-Roads Platform, Working Group 2 Technical Aspects.

Data for Road Safety, 2021, Privacy Statement - Data for Road Safety. Available at: https://www.dataforroadsafety.eu/images/Documenten/20210706_Privacy_Statement._DFRS_ecosystem.pdf (Accessed: 24 February 2025).

Data Protection Act 1050/2018, 2018. Available at: https://finlex.fi/fi/laki/ajantasa/2018/20181050 (Accessed: 20 February 2025).

De Luca, S., 2024. The path to 6G. European Parliamentary Research Service Briefing. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757633/EPRS_BRI%282024%29757633_EN.pdf

ETSI TS 102 940, 2021, Technical Specification "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2". Available at: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf

ETSI TS 102 941, 2022. Intelligent Transport Systems (ITS); Trust and Privacy Management, v.2.2.1. ETSI. Available at: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/02.02.01_60/ts_102941v020201p.pdf (Accessed: 23 February 2025).

ETSI TS 103 097, 2022. Intelligent Transport Systems (ITS); Security header and certificate formats, v.2.1.1. ETSI. Available at: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/02.01.01_60/ts_103097v020101p.pdf (Accessed: 23 February 2025).

EU 2002/58, 2002, Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24120 (Accessed: 20 February 2025).

EU 2010/40/EU, 2010, Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Available at: https://eur-lex.europa.eu/eli/dir/2010/40/oj/eng

EU 2016/588, 2016, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 14 September 2016, ”5G for Europe: An Action Plan”. Available at: https://digital-strategy.ec.europa.eu/en/library/communication-5g-europe-action-plan-and-accompanying-staff-working-document (Accessed 30 December 2024).

EU 2016/679, 2016, Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#cpt_IV (Accessed: 20 February 2025).

EU 2021/118, 2021, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 9 March 2021."2030 Digital Compass: the European way for the Digital Decade". Available at: https://commission.europa.eu/document/download/9fc32029-7af3-4ea2-8b7a-4cd283e8e89e_en?filename=cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf&prefLang=en

EU 2022/2557, 2022, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

EU 2023/2661, 2023, Directive (EU) 2023/2661 of the European Parliament and of the Council of 30 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302661

EU C/2016/766, 2016, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 30 November 2016. "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0766&from=FR

EU C/2019/1789, 2019, Commission Delegated Regulation C(2019) 1789 of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282019%291789

EU C/2024/6798, 2024. Commission Implementing Decision of 12 November 2024 establishing a working programme for Directive 2010/40/EU for the period 2024-2028. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/C/2024/6798/oj

EU Open Source Strategy 2020–2023, 2020, European Commission, Communication to the Commission, Open Source Software Strategy 2020–2023, Think Open, Brussels 21.10.2020 C(2020) 7149 Final. Available at: https://commission.europa.eu/about/departments-and-executive-agencies/digital-services/open-source-software-strategy_en

European Commission, 2022, 5G Coverage along Transport Corridors: first wave of projects selected for co-funding 5G corridor infrastructures, official website of the European Union. Website. Published 22 December 2022. Available at: https://digital-strategy.ec.europa.eu/fi/news/5g-coverage-along-transport-corridors-first-wave-projects-selected-co-funding-5g-corridor (Accessed: 30 December 2024).

European Data Protection Board (2021) Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 2.0. Adopted on 9 March 2021. Available at: https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf (Accessed: 23 February 2025).

Export cluster (Vientiklusteri), n.d. Fintraffic. Website. Available at: https://www.fintraffic.fi/fi/liikenteendataekosysteemi/vientiklusteri (Accessed: 20 January 2025).

FCC C-V2X Auto Safety Spectrum Rules, 2024, Federal Communication Commission Washington, D.C. 20554 In the Matter of Use of the 5.850-5.925 GHz Band ET Docket No. 19-138, Second Report and Order, Adopted November 20, 2024, Released November 21, 2024. Available at: https://www.fcc.gov/document/fcc-adopts-c-v2x-auto-safety-spectrum-rules

Finnish Government, 2023. "A strong and committed Finland: Programme of Prime Minister Petteri Orpo's Government, 20 June 2023”. Publications of the Finnish Government 2023:58. Available at: https://julkaisut.valtioneuvosto.fi/handle/10024/165042

Finnish Government, 2024. ”Valtakunnallinen liikennejärjestelmäsuunnitelma vuosille 2026–2037” (The National Transport System Plan for 2026-2037). Publications of the Finnish Government 2024:XX. Draft plan. Available at: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=47f126a9-4eea-43c5-a4ba-c57137827636

Fintraffic interview, 2024, Teams, 28 August 2024, Subject:” The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of C-ITS central units, the progress of this subject in Fintraffic Tie Oy”

IETF RFC 5280, 2008, Internet Engineering Task Force (IETF) Network Working Group Request for Comments 5280, May 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Available at: https://datatracker.ietf.org/doc/html/rfc5280

IETF RFC 8446, 2018, Internet Engineering Task Force (IETF) Request for Comments 8446 ISSN 2070-1721, August 2018, The Transport Layer Security (TLS) Protocol Version 1.3. Available at: https://datatracker.ietf.org/doc/html/rfc8446

Intens interview, 2024, Teams, 30 October 2024, Subject:” The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of C-ITS central units, the similar progress in Czech Republic”

ISO 17427-1, 2018, ”Intelligent transport systems. Cooperative ITS. Part 1: Roles and responsibilities in the context of the co-operative ITS architecture(s) (ISO 17427-1:2018), Available at: https://www.iso.org/standard/66924.html (subject to a fee)

ISO/IEC 15408-1, 2022, ”Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1 Introduction and general model”, reference number ISO/IEC 15408-1:2022(E), Available at: https://www.iso.org/standard/72891.html (subject to a fee)

ISO/IEC 19464, 2014, ISO/IEC 19464:2014 Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification, Published (Edition 1, 2014), standard subject to a fee.

Kilpiö, V., Kotilainen, I., Kulmala, R., Rantanen, J., Nieminen, J., Hönö, S-V., Kynsijärvi, N., Mäkipää, M., Paaso-Rantala, H., 2024. ”Utilisation of commercial mobile networks in the deployment of C-ITS services”. Traficom Research Reports 11/2024. Available at: https://www.traficom.fi/sites/default/files/media/file/C-ITS-mobiili-loppuraportti_11_2024.pdf

Kotilainen, I., Scholliers, J., Öörni, R., Kulmala, R., 2023. ”Viranomaisen roolit vuorovaikutteisten älykkäiden liikennejärjestelmien (C-ITS) palveluiden käyttöönotossa ja operatiivisessa käytössä” (The roles of the authorities in the implementation and operational use of Cooperative Intelligent Transport Systems (CITS) services). Traficom Research Reports 23/2023. Available at: https://www.traficom.fi/sites/default/files/media/file/C-ITS-roolit_raportti_final.pdf

Kynsijärvi, N., Majala, T., Scholliers, J., Kauvo, K. & Lehtonen, S., 2024. “Piloting cybersecure and interoperable cellular C-ITS services”. Traficom Research Reports 12/2024. Available at: https://www.traficom.fi/sites/default/files/media/publication/2024%2005%2029%20C-ITS%20pilot%20final%20report.pdf

Laine, T. & Kotilainen, I., 2024. ”RTTI-asetuksen ja ITS-direktiivin päivityksen velvoitteista ja toimijoiden rooleista” (Report on the obligations and roles imposed by the European Commission’s updated RTTI Regulation and ITS Directive). Traficom Research Reports 20/2024. Available at: https://www.traficom.fi/sites/default/files/media/publication/RTTI-asetus%20raportti%2020_2024.pdf

Linux Foundation, 2024, Open Source Guides - Setting an Open Source Strategy. Website. Available at: https://www.linuxfoundation.org/resources/open-source-guides/setting-an-open-source-strategy (Accessed: 12 February 2025).

LVM/2021/137, 2021, Government resolution on the promotion of transport automation. Available at: https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80772030

Maerivoet, S. & Ons, B., 2023. Draft report on connected vehicle deanonymisation research review and impact study. Trusted Integrity and Authenticity for Road Applications (TIARA) - CEDR Call 2022 Data: Integrity, Authenticity, and Non-Repudiation integrated in Trust Models for CITS applications. Draft report. Available at: https://www.cedr.eu/docs/view/671a142d82dd7-en (Accessed: 21 February 2025)

Menezes, A., van Oorschot, P., Vanstone, S., 1996, The Handbook of Applied Cryptography. Available at: https://cacr.uwaterloo.ca/hac/about/chap1.pdf

Microsec and Commsignia interview, 2024, Teams, 29 August 2024, Subject: ”The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of root certificate authorities, the service portfolio of Microsec relating PKI services”.

Miettinen, K., Miettinen, A., Hauta, J., Töyrylä, S., Reinimäki, S., 2021. ”Liikenteen automaation lainsäädäntö- ja avaintoimenpidesuunnitelma” (Action plan on legislation and key measures of transport automation). Publications of the Ministry of Transport and Communications 2021:28. Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163629/LVM_2021_28.pdf?sequence=1&isAllowed=y

Ministry of Transport and Communications, 2024, Sustainable growth, wellbeing, safety and security through data and future-proof connections. Group strategy for the administrative branch of the Ministry of Transport and Communications. Publications of the Ministry of Transport and Communications 2024:3. Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165418/LVM_2024_3.pdf?sequence=1&isAllowed=y

Monotch interview, 2024, Teams, 21 August 2024, Subject: ”The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of C-ITS central units, the similar progress in Netherlands”.

OASIS AMQP Protocol Specification, 2012, OASIS Standard Advanced Message Queuing Protocol (AMQP) Version 1.0, 29 October 2012, Available at: https://www.amqp.org/resources/download

Office of the Data Protection Ombudsman (n.d.) *Impact assessments*. Website. Available at: https://tietosuoja.fi/vaikutustenarviointi (Accessed: 20 February 2025).

Office of the Data Protection Ombudsman (n.d.) *Personal data breaches*. Website. Available at: https://tietosuoja.fi/tietoturvaloukkaukset (Accessed: 20 February 2025).

Office of the Data Protection Ombudsman (n.d.) *Pseudonymised and anonymised data.* Website. Available at: https://tietosuoja.fi/pseudonymisointi-anonymisointi (Accessed: 20 February 2025).

Office of the Data Protection Ombudsman (n.d.) *Risk assessment and data protection planning*. Website. Available at: https://tietosuoja.fi/arvioi-riskit (Accessed: 20 February 2025).

Office of the Data Protection Ombudsman (n.d.) *Safeguards to supplement transfer tools*. Website. Available at: https://tietosuoja.fi/tiedonsiirtovalineita-taydentavat-suojatoimet (Accessed: 20 February 2025).

Office of the Data Protection Ombudsman (n.d.) *Transfers of personal data out of the European Economic Area*. Website. Available at: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle (Accessed: 20 February 2025).

Office of the Data Protection Ombudsman (n.d.) *When is the processing of personal data permitted?*. Website. Available at: https://tietosuoja.fi/kasittelyperusteet (Accessed: 20 February 2025).

Rekola, M., Kolinen, L., Asikainen, E., Heliste, L., Immonen, E., Starck, M., Ahokas, M., Suomento, J., Johansson, S., 2022. ”Liikenneturvallisuusstrategia 2022–2026” (Traffic Safety Strategy 2022–2026). Publications of the Ministry of Transport and Communications 2022:3. Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163951/LVM_2022_3.pdf?sequence=1&isAllowed=y

Swarco interview, 2024, Teams, 22 October 2024, Subject:” The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of C-ITS stations”.

TEN-TEC central C-ITS stations in EU countries, 2025, European Commission TENtec Version 6.1.0 (Filter: C-ITS Stations & Networks). Website. Available at: https://webgate.ec.europa.eu/tentec-maps/web/public/screen/home (Accessed: 24 February 2025).

Teskalabs interview, 2024, Teams, 5 September 2024, Subject: "The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of root certificate authorities, the service portfolio of Teskalabs relating PKI services”

Thales Luna HSMs, n.d. Thales Luna HSM’s High Assurance Hardware Security Modules (Features tab). Website. Available at: https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms (Accessed: 24 February 2025).

Traficom, 2024. Call for tenders: "Liikenne- ja viestintävirasto 525852 / C-ITS-palveluiden tarve ja priorisointi Suomessa - Liikenne- ja viestintävirasto Traficom - Älyliikenteen, automaation ja liikkumispalveluiden asiantuntijapalvelut (DPS), sisäinen kilpailutus (DPS)" [Finnish Transport and Communications Agency 525852 / The needs for and prioritization of C-ITS services in Finland - Finnish Transport and Communications Agency - Expert services for intelligent transport, automation and mobility services (DPS), internal terndering (DPS)], date 9 September 2024.

UN Regulation No. 155, 2021, United Nations, "Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations, Addendum 154 – UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system", E/ECE/TRANS/505/Rev.3/Add.154. Available at: https://unece.org/sites/default/files/2023-02/R155e%20%282%29.docx

Vegvesen interview, 2024, Teams, 8 October 2024, Subject: "The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of C-ITS central units, the similar progress in Norway"

Viswanathan, H. & Mogensen, P., 2023. Communications in the 6G Era. Espoo: Nokia Bell Labs White Paper. Available at: https://www.nokia.com/asset/207766

Yue, X., Zeng, S., Wang, X., Yang, L., Bai, S. ja He, Y., 2022 'A practical privacy-preserving communication scheme for CAMs in C-ITS', Journal of Information Security and Applications, 65, 103103. Available at: https://doi.org/10.1016/j.jisa.2021.103103

Öörni, R., 2024, Network effects in C-ITS – an analysis approach based on conditional probability and system characteristics, European Transport Research Review (2024) 16:73. Available at: https://doi.org/10.1186/s12544-024-00694-6

Finnish Transport and Communications Agency Traficom
PO Box 320, FI-00059 TRAFICOM
Switchboard: +358 29 534 5000
traficom.fi

ISBN 978-952-311-985-7
ISSN 2669-8781 (e-publication)

TRAFICOM
Finnish Transport and Communications Agency