TRAFICOM
Liikenne- ja viestintävirasto

C-ITS-järjestelmän toteutusmalli ja käyttöönoton edellytykset Suomessa

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

C-ROADS

Euroopan unionin osarahoittama

Traficomin tutkimuksia ja selvityksiä
Traficoms forskningsrapporter och utredningar
Traficom Research Reports

18/2025

TRAFICOM
Liikenne- ja viestintävirasto

Julkaisupäivämäärä
6.5.2025

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) 978-952-311-980-2

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	Raportin kieli	Luottamuksellisuus	Kokonaissivumäärä
Risto Öörni	suomi	julkinen	182

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

TRAFICOM
Transport- och kommunikationsverket

Utgivningsdatum
6.5.2025

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) 978-952-311-980-2

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	Språk	Sekretessgrad	Sidoantal
Risto Öörni	finska	offentlig	182

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

TRAFICOM
Finnish Transport and Communications Agency

Date of publication
6 May 2025

Title of publication
Implementation model and deployment preconditions for C-ITS 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) 978-952-311-980-2

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	Language	Confidence status	Pages, total
Risto Öörni	Finnish	Public	182

Distributed by	Published by
Finnish Transport and Communications Agency Traficom	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.

Helsinki, 6. toukokuuta 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.

Helsingfors, den 6 maj 2025

Risto Öörni
Specialsakkunnig
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.

Helsinki, 6 May 2025

Risto Öörni
Special Adviser
Finnish Transport and Communications Agency Traficom

Sisällysluettelo

Lyhenteet ja sanasto

3GPP	Standardointijärjestöistä ja markkinatoimijapartnereista koostuva matkaviestinverkkoteknologioihin perustuvien teknologioiden kehittämiseen keskittyvä organisaatio (Third Generation Partnership Project).
AA	Valtuuttaja, jonka avulla C-ITS-yksiköt valtuutetaan tarjoamaan tiettyjä C-ITS-palveluita C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisissa C-ITS-järjestelmissä (Authorization Authority).
AMQP	Avoin taustajärjestelmien välillä suurta tiedonsiirron skaalautuvuutta ja luotettavuutta tukeva tiedonsiirtoprotokolla (Advanced Message Queuing Protocol).
API	Laitteiden ja ohjelmistojen välisen viestinnän mahdollistama ohjelmoitava rajapinta (Application Programming Interface).
AT	C-ITS-yksiköille luovutettava valtuutuslippu (Authorization Ticket).
BI	C-ITS-järjestelmien pitkän kantaman tiedonsiirrossa taustajärjestelmien väliseen tiedonvaihtoon tarkoitettu protokolla (Basic Interface).
CAM	Ajonevojen sijainti-, suunta- ja nopeustietoja sisältämä C-ITS-viesti (Cooperative Awareness Message).
CCAM	Verkottunut ja automatisoitunut liikenne (Cooperative Connected Automated Mobility).
CCMS	EU:n C-ITS-turvatunnusten hallintajärjestelmä (C-ITS Security Credential Management System).
C-ITS	Vuorovaikutteisten älykkäiden liikennejärjestelmien välityksellä tarjottavat suojatut ja luotetut älyliikenteen palvelut (Cooperative Intelligent Transport Systems).
C-ITS-toimija	C-ITS-järjestelmän toimintaan liittyvät organisaatiot ja henkilöt, joiden roolit ja vastuut määritellään ISO-standardissa 17427-1.
C-V2X	Vuorovaikutteisten älykkäiden liikennejärjestelmien viestintään tarkoitetut 3GPP-yhteistyöjärjestön matkaviestinverkkoteknologiaan kehittämät kommunikointitavat (Cellular Vehicle-to-Everything).
CPA	C-ITS-varmennepolitiikkaviranomainen (Certificate Policy Authority).
CPOC	C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen C-ITS-yhteyspiste (C-ITS Point of Contact).
CPS	C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) juurivarmentajilta vaadittu varmennekäytäntöjen kuvaus (Certificate Practise Statement).
CSMS	Kyberturvallisuuden hallintajärjestelmä (Cyber Security Management System)
DATEX2	Liikennejärjestelmien väliseen tiedonvälitykseen ja -vaihtoon tarkoitettu eurooppalainen standardi (DATa EXchange).

DDoS	Internet-verkossa useista lähteistä tapahtuva palvelunestohyökkäys (Distributed Denial-Of-Service).
DENM	Liikenteen ja tieverkon tilasta sekä häiriötilanteista tietoa välittävä C-ITS-viesti (Decentralized Environmental Notification Message).
DfRS	SRTI-tietojen hyödyntämistä edistävä eurooppalainen ekosysteemi (Data for Road Safety).
DNS	Internet-verkossa toimiva nimipalvelujärjestelmä, joka ylläpitää tietoja verkossa sijaitsevien palveluiden IP-osoitteista ja osoitteisiin liitetyistä nimistä (Domain Name System)
EA	Valtuuttaja, jonka avulla C-ITS-yksiköt rekisteröidään osaksi C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaista C-ITS-palvelutoteutusta, (Enrollment Authority).
EAL	Standardin ISO 15408 mukainen IT-järjestelmän tai tuotteen tietoturvallisuuden tason luokitus (Evaluation Assurance Level).
ECTL	C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen luotettujen PKI-varmenteiden luettelo (European Certificate Trust List).
EDPB	Euroopan tietosuojaneuvosto (European Data Protection Board).
ETSI	Eurooppalainen telealan standardisoimisjärjestö. (European Telecommunications Standards Institute).
EU Root CA	C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen juurivarmennepalveluiden tuottaja (EU Root Certificate Authority).
GDPR	EU:n yleinen tietosuoja-asetus (General Data Protection Regulation).
HSM	Fyysinen laite, jota käytetään tietoturvallisuutta vaativissa sovelluksissa salausavainten turvalliseen säilytykseen ja käyttöön, esim. C-ITS-yksiköt (Hardware Secure Module).
IEC	Kansainvälinen sähköalan standardointijärjestö (International Electrotechnical Commission).
IEEE	Kansainvälinen esimerkiksi langattoman Ethernet-verkon standardin 802.11 julkaissut järjestö (Institute of Electrical Engineers).
IETF	Internet-protokollien standardoinnista vastaava organisaatio (Internet Engineering Task Force).
II	C-ITS-järjestelmien tiedonsiirrossa tiedonvaihtopalvelimien väliseen tiedonvaihtoon tarkoitettu protokolla (Improved Interface).
IP	Pakettikytkentäisissä verkoissa käytettävä protokolla, joka mahdollistaa verkkoon kytkettyjen laitteiden viestinnän keskenään (Internet Protocol).

ISMS	Tietoturvallisuuden hallintajärjestelmä (Information Security Management System).
ISO	Kansainvälinen standardointijärjestö (International Organization for Standardization).
ISO 27001	ISO-standardointijärjestön julkaisema ja ylläpitämä tietoturvallisuuden standardi, joka asettaa vaatimukset organisaation tietoturvallisuuden hallintajärjestelmälle.
ITS-G5	C-ITS-järjestelmissä käytettävä radioteknologiaan ja IEEE:n langattomien verkkojen 802.11-standardisarjaan perustuva lyhyen kantaman tiedonsiirtoon Euroopassa käytetty nimitys.
JRC	Euroopan unionin Italian Isprassa sijaitseva yhteinen tekninen tutkimuskeskus (Joint Research Centre).
NAP	Liikkumispalveluiden tuottajille ja kehittäjille tarkoitettu digitaalisessa muodossa säilytettävien oleellisten liikkumistietojen kansallinen yhteyspiste (National Access Point).
NIS	Euroopan unionin verkko- ja tietoturvadirektiivi (Network and Information Systems).
OASIS	Teollisuuden ja julkisen sektorin toimijoista sekä tutkimusorganisaatioista koostuva mm. AMQP-protokollan kehittänyt ja julkaissut organisaatio (Organization for the Advancement of Structured Information Sharing).
OBU	C-ITS-ajoneuvoyksikkö (On-Board Unit).
OSI-malli	Tiedonsiirtoyhteyksien toiminnan seitsemässä eri kerroksessa kuvaava ITU-T-standardointijärjestön standardoima referenssimalli (Open Systems Interconnection).
PKI	Julkisen avaimen infrastruktuuri, joka on tietotekniikassa käytetty varmennemenetelmä (Public Key Infrastructure).
PP	C-ITS-yksikön turvaprofiili, joka määrittelee standardin ISO 15408 mukaisen tietoturvallisuuden evaluoinnin laajuuden (Protection Profile).
Quadtree	Yleisesti paikkatietojärjestelmissä käytetty tietorakenne.
RCA	C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen juurivarmentaja (Root Certificate Authority).
RTTI	Tosiaikainen liikennetieto (Real-Time Traffic information), josta on säädelty Euroopan komission delegoidussa asetuksessa 2022/670.
SaaS	Ohjelmistojen tarjoaminen palveluna (Software as a Service).
SLA	Palvelutasosopimus (Service Level Agreement).
SOG-IS	Tietojärjestelmien turvallisuuteen keskittyvä eurooppalainen yhteistyöelin (Senior Officials Group on Information Systems Security).

SPAT	Liikennevalojen tilatietoja lähettävä C-ITS-viesti (Signal Phase and Timing).
SREM	Liikennevalojen etuuspyyntöihin tarkoitettu C-ITS-viesti (Signal Request Extension Message).
SRTI	Liikenneturvallisuuteen liittyvät yleiset vähimmäisliikennetiedot (Safety-Related Traffic Information). Tietosisältö on määritelty Euroopan komission delegoidussa asetuksessa 886/2013.
SSEM	Liikennevalojen etuuspyynnön vastaanottoviesti (Signal request Status Extension Message).
SSP	Palvelukohtaiset luvat (Service Specific Permissions).
RSU	C-ITS-tienvarsiyksikkö (Road-Side Unit).
TCP/IP	Internet-verkon liikennöinnissä yleisesti käytettävä kahden protokollan yhdistelmä, joista IP-protokolla yksilöi laitteen ja TCP-protokolla käytettävän sovelluksen portin (Transport Control Protocol / Internet Protocol).
TIA	GDPR:n mukainen menetelmä siirtovaikutusten ja kohdemaan tietosuojan tason arviointiin henkilötietojen siirrossa EU- tai ETA-alueen ulkopuolelle (Transfer Impact Assessment).
TLM	Luotetun luettelon hallinnoija on C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen toimija, joka huolehtii hyväksyttyjen juurivarmentajien ja juurivarmenteiden luettelosta (Trust List Manager).
TLS	Internet-verkossa viestien eheyden varmistamiseen ja käyttäjien autentikointiin käytettävä salausprotokolla (Transport Layer Security).
TOE	Standardin ISO 15408 mukainen IT-järjestelmän tai tuotteen tietoturvallisuuden tason arvioinnin laajuuden määrittely (Target Of Evaluation).
UN R155	UNECE:n valmistelema vuonna 2021 voimaan tullut ajoneuvojen kyberturvallisuutta koskeva säädös (UN Regulation No. 155).
UNECE	YK:n Euroopan alueen talouskomissio (The United Nations Economic Commission for Europa).
X.509	Kryptografinen ITU-T-standardointijärjestön julkaisema standardi julkisen avaimen salauksessa käytettäville varmenteille.

1 Johdanto

1.1 Tausta ja tavoitteet

Suomessa älykkäiden liikennejärjestelmien palveluita on jo useiden vuosien ajan kehitetty ja kokeiltu tieliikenteen viranomaisten toimesta niin kansallisesti kuin muidenkin maiden kanssa yhteistyössä. C-ITS-palveluilla (Cooperative Intelligent Transport Systems) tarkoitetaan älykkäiden liikennejärjestelmien palveluita, jotka toteutetaan vuorovaikutteisesti eri järjestelmien välillä vaihtamalla standardoituja tosiaikaisia C-ITS-viestejä, joiden luotettavuus taataan EU:n C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) avulla. Viestejä voidaan jakaa ajoneuvojen, infrastruktuurin ja muiden tienkäyttäjien kesken. C-ITS-palveluita voidaan toteuttaa pitkän- tai lyhyen kantaman tiedonsiirrolla. Eurooppalaisten jäsenmaiden ja tienpitäjien yhteistyöryhmä C-Roads on määritellyt lyhyen kantaman tiedonsiirtoon radioverkkoihin (ITS-G5) ja pitkän kantaman tiedonsiirtoon IP-verkkoihin pohjautuvaa toteutusta. Toteutusta, joka tukee sekä lyhyen- että pitkän kantaman tiedonsiirtoa, kutsutaan hybridikommunikaatioksi.

Suomessa on C-ITS-palveluiden toteutuksessa sitouduttu noudattamaan olemassa olevia C-ITS-standardeja sekä C-Roads Platform -yhteistyöryhmän määritelmiä. Kansallisen toteutusmallin kannalta merkittävä osa on pohjana toimiva tiedonsiirtoratkaisu, sillä lyhyen- ja pitkän kantaman tiedonsiirtoon käytetyt järjestelmät eroavat toisistaan moneltakin osin. Yhteistä molemmissa toteutusmalleissa on kuitenkin EU:n C-ITS-turvallisuus- ja varmennepolitiikkojen asettamat vaatimukset. Suomi ja muut Pohjoismaat ovat keskittyneet erityisesti matkaviestinverkon hyödyntämiseen C-ITS-järjestelmien tiedonsiirtoratkaisuna. Aiheeseen liittyvää tutkimus- ja kehitystyötä on tehty maiden välillä mm. EU-komission tukemassa NordicWay-projektissa.

Suomen viranomaisten tavoitteena on luoda edellytyksiä C-ITS-palveluiden käyttöönotolle. Varsinaista velvoittavaa lainsäädäntöä C-ITS-palveluiden toteuttamiseen, toteutuksen johtamiseen tai hallinnointiin ei nykyisellään kuitenkaan ole voimassa. Aiemmin Euroopan komissio ja jäsenvaltiot ovat valmistelleet ja julkaisseet asetusehdotuksen vuorovaikutteisista älykkäiden liikennejärjestelmien palveluista, jota ei kuitenkaan saatettu voimaan. Muuta sääntelyä ja standardointia on C-ITS-palveluiden järjestämiseen liittyen kuitenkin laajasti olemassa muun muassa viestien rakenteesta ja profiileista, toimijoiden rooleista ja vastuista, C-ITS-yksiköistä ja C-ITS-turvatunnusten hallintajärjestelmästä (EU CCMS) sekä kyberturvallisuudesta ja tietosuojasta.

Vuosina 2023–2024 Suomessa toteutettiin C-ITS-projekteja, jotka tarkastelivat osapuolten rooleja, vertailivat eri teknologioita ja arvioivat matkaviestinverkkojen kyvykkyyttä C-ITS-palveluiden toteuttamisessa. Niissä ei kuitenkaan pyritty muodostamaan yksityiskohtaisempaa kuvausta kansallisesta toteutusmallista tai konkreettisemmista toimenpiteistä. Tämän selvitystyön tavoitteena oli valmistella C-ITS-palveluiden arkkitehtuurin toteutusmallia Suomessa sekä luoda edellytyksiä C-ITS-palveluiden käyttöönotolle huomioiden EU:n C-ITS:n turvallisuus- ja varmennepolitiikan asettamat vaatimukset sekä kansallisen tahtotilan.

1.2 Työn rajaukset

C-ITS-palveluiden yhteiskuntataloudellisuuden arviointi sekä eri tiedonsiirtoteknologioiden soveltuvuus palveluiden tuottamiseksi rajattiin tämän työn tarkastelun ulkopuolelle.

Raportti ei ota kantaa C-ITS-palveluiden yhteiskuntataloudellisuuteen

Tässä työssä tunnistettiin C-ITS-palveluiden käyttöönottoon liittyviä kustannuksia, jotka aiheutuvat mm. EU:n C-ITS:n turvallisuus- ja varmennepolitiikoiden vaatimuksista. Näitä kustannuksia käsitellään tarkemmin luvussa 5.7, jonka mukaisesti ne muodostuvat seuraavista osa-alueista:

- kansallisen C-ITS-keskusyksikön ja tiedonvaihtopalvelimen käyttöönotto ja operointi
- juurivarmennepalvelut, keskitetyn kansallisen juurivarmennepalvelun perustaminen ja varmennepalveluiden käyttö
- C-ITS-yksikköoperaattoreille syntyvät kustannukset turvallisuus- ja varmennepolitiikan vaatimuksiin liittyen.

C-ITS-palveluiden toteuttaminen aiheuttaa myös muita kustannuksia, jotka voivat liittyä esimerkiksi palveluiden vaatimien lähtötietojen tuottamiseen tai palveluiden tarjoamiseen loppukäyttäjille. Tässä raportissa ei arvioida näiden kustannusten suuruusluokkaa tai jakautumista eri toimijoiden kesken. Raportissa ei myöskään ole arvioitu C-ITS-palveluiden vaikutuksia eikä siten niiden yhteiskuntataloudellista kannattavuutta Suomessa, mikä on yleisesti lähtökohtana julkisen rahan investoinneille. Jotta C-ITS-palveluiden toteutusta ja käyttöönottoa voitaisiin varauksetta suositella, vaatisi se tarkempaa hyöty-kustannusanalyysia. Tällaisen analyysin toteuttaminen ei kuitenkaan ollut osana tätä selvitystyötä, mutta se on suositeltava jatkotutkimusaihe. C-ITS-palveluiden tarpeeseen ja priorisointiin liittyen on tämän raportin kirjoittamishetkellä kilpailutettu erillinen hanke, jonka keskeisimpinä tavoitteina on tuottaa tietoa C-ITS-palveluihin liittyvistä käyttäjien ja yhteiskunnan tarpeista sekä laatia ehdotus ensi vaiheessa Suomessa toteutettavista C-ITS-palveluista ja priorisoida palvelut toisiinsa nähden (Traficom 2024). Nämä tulokset eivät ole olleet saatavilla vielä tämän raportin valmistumishetkellä.

Raportti ei ota kantaa eri tiedonsiirtoteknologioiden soveltuvuuteen yksittäisten C-ITS-palveluiden tuottamiseksi

Tämä selvitystyö ei tarkastele eri tietoliikenteen teknologioiden soveltuvuutta C-ITS-palveluiden toteuttamisen suhteen. Luvussa 6.2 käsitellään C-ITS-viestien välittämiseen käytettävien tiedonsiirtoteknologioiden yleiskuvausta sekä käydään yleisellä tasolla läpi C-Roads-yhteistyöfoorumin tunnistamat teknologiat: lyhyen ja pitkän kantaman tiedonsiirto sekä hybridiratkaisu. Tämä raportti keskittyy varsinaisesti niihin osa-alueisiin, joilla EU:n C-ITS-turvatunnusten hallintajärjestelmä on voimassa, jolloin koko palveluketjun toteutusmallin suhteen jää tiettyjä vapausasteita, esimerkiksi tienpitäjille tietojen tuottamiseen sekä palveluntarjoajille tietojen välittämiseen loppukäyttäjille. Selvitystyössä keskityttiin pitkän kantaman tiedonsiirtoon perustuvan toteutuksen kuvaukseen, jolloin myöskään varsinaista vertailua lyhyen ja pitkän kantaman toteutusten välillä ei tehdä, vaan eroavaisuuksia nostetaan raportissa esiin tarpeen mukaan. Edellä mainitun kaltaisen tarkastelun tekeminen voi kuitenkin olla perusteltua, kuten luvussa 9 myöhemmin

todetaan. Yleisemmällä tasolla eri tiedonsiirtoteknologioiden kyvykkyyttä C-ITS-palveluiden toteutuksessa on tutkittu erillisissä selvityksissä (katso esimerkiksi Kilpiö et al. 2024 sekä Kynsijärvi et al. 2024).

2 Menetelmät

Työn tutkimusmenetelminä olivat kirjallisuuskatsaus, yhteistyö ohjausryhmässä, asiantuntijahaastattelut sekä työpajatyöskentely. Keskeisenä menetelmänä oli lisäksi tilaajien, toimittajien sekä ohjausryhmän jäsenten asiantuntijaosaamisen hyödyntäminen.

Kirjallisuuskatsaus pohjautui erityisesti Euroopan unionin yhteisen teknisen tutkimuskeskuksen (Joint Research Centre, JRC) julkaisemiin C-ITS-turvallisuus- ja varmennepolitiikkadokumentteihin sekä C-Roads-yhteistyöfoorumin julkaisemiin määritelmiin. Lisäksi työssä hyödynnettiin kattavasti aiempia C-ITS-kehityksestä ja -käyttöönotosta tehtyjä tutkimuksia ja selvityksiä.

Tärkeänä tutkimusmenetelmänä hyödynnettiin myös asiantuntijahaastatteluita, joiden avulla kartoitettiin usean eri maan kaupallisten toimijoiden ratkaisujen yhteentoimivuutta eurooppalaisen C-ITS-politiikan kanssa. Näkökulmia haettiin myös julkisen sektorin toimijoilta, jotka ovat päättäneet itse panostaa C-ITS-kehitykseen.

Työn aikana järjestettiin yksi työpaja kansallisten sidosryhmätoimijoiden kanssa, jossa haettiin näkökulmia kansalliseen tahtotilaan C-ITS-toteutuksen edistämiseksi sekä arvioitiin eri vaihtoehtojen toimivuutta C-ITS-palvelutoteutuksen arkkitehtuurin osien toteuttamiseksi.

Selvitystyön aikana ohjausryhmä kokoontui neljä kertaa. Ohjausryhmässä olivat edustettuina C-ITS-kehityksen näkökulmasta valtionhallinnon sekä kuntasektorin keskeiset toimijat. Ohjausryhmän tärkeimpänä tehtävänä oli seurata ja ohjata työn edistymistä.

3 EU:n C-ITS-turvallisuus- ja varmennepolitiikka

3.1 Tausta

C-ITS-palveluiden eurooppalainen yhteinen turvallisuus- ja varmennepolitiikka on alun perin luotu vuosina 2014–17 osana Euroopan komission perustamien C-ITS-yhteistyöfoorumien työtä (C-ITS Deployment Platform ja C-ITS Platform). Laajemmin foorumien ja komission organisoiman työn tavoitteena oli edistää C-ITS-palveluiden käyttöönottoa luomalla tärkeimpien eurooppalaisten sidosryhmien kanssa yhteiset periaatteet rajojen yli yhteentoimivien C-ITS-palveluiden käyttöönotolle Euroopassa. C-ITS Deployment Platform -foorumin loppuraportilla oli merkittävä rooli komission vuonna 2016 laatimaan eurooppalaiseen strategiaan vuorovaikutteisten, yhdistettyjen ja automatisoitujen ajoneuvojen käyttöönottoon liittyen (EU C/2016/766). C-ITS-foorumien määrittely- ja suunnittelutyön tuloksena ensimmäinen C-ITS-palveluiden turvallisuus- ja varmennepolitiikka on julkaistu vuonna 2017.

C-ITS-turvallisuus- ja varmennepolitiikan tavoitteena on varmistaa C-ITS-yksiköiden välisen viestinnän tietoturvallisuus, kuten viestien luottamuksellisuus ja eheys sekä yksiköiden ja niiden käsittelemän tiedon tietoturvallinen hallinta. Viestinnän turvallisuus perustuu C-ITS-varmennepolitiikassa määriteltyyn julkisen avaimen menetelmään (PKI, Public Key Infrastructure) ja C-ITS-järjestelmien eurooppalaiseen luottamusmalliin. C-ITS-yksiköiden tietoturvallinen hallinta varmistetaan turvallisuuspolitiikassa asetetuilla hallintaan liittyvillä vaatimuksilla. Nämä vaatimukset ja periaatteet muodostavat EU:n yhteisen C-ITS-palveluiden turvallisuus- ja varmennepolitiikan.

Turvallisuus- ja varmennepolitiikan seuraavat versiot (2.0) esiteltiin osana Euroopan komission C-ITS-palveluiden delegoitua asetusehdotusta vuonna 2019 (EU C/2019/1789). Vaikka varsinaista delegoitua asetusehdotusta ei hyväksyttykään lopullisessa Euroopan unionin neuvoston äänestyksessä, niin kaikki asianosaiset sidosryhmät olivat hyväksyneet C-ITS-turvallisuus- ja varmennepolitiikan periaatteet jo ennen asetusehdotuksen julkaisua (EU C/2019/1789, 13). Tämän erillisen hyväksynnän myötä Euroopan komissio aloitti C-ITS-palveluiden käyttöönoton edistämisen C-ITS-turvallisuus- ja varmennepolitiikan periaatteiden mukaisilla tavoilla. Toimissa keskityttiin erityisesti C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) keskeisten elementtien valmisteluun sekä pilottitarkoituksiin perustettavan EU-juurivarmennepalvelun (EU Root Certificate Authority, EU Root CA) toteutukseen.

EU:n hallinnoiman juurivarmennuspalvelun tuottamisesta järjestettiin kilpailutus keväällä 2019 (JRC/IPR/2019/OP/0365). Kilpailutuksen voitti ranskalainen digitaalisten identiteettien hallintapalveluihin keskittynyt IDnomic. Jo ennen varsinaisen sopimuksen solmimista vuoden 2019 lopussa IDnomic siirtyi yrityskaupan myötä Atos SE:n omistukseen, joka tuottaa tälläkin hetkellä kyseistä palvelua. Raportin kirjoittamisen aikana käytössä olivat sopimuksen optiovuodet. Sopimuksen mukaisesti palvelua jatketaan vuoden 2022 jälkeen vuosittain enintään vuoden 2026 loppuun saakka.

Euroopan komissiossa C-ITS-turvallisuus- ja varmennepolitiikkaa on C-ITS-foorumien tekemän työn jälkeen kehitetty Euroopan unionin Italiassa Isprassa sijaitsevan yhteisen teknisen tutkimuskeskuksen (Joint Research Centre, JRC) johdolla.

JRC:n tehtävänä on tarjota riippumatonta tieteellistä ja teknistä tukea Euroopan unionin päätöksenteon tueksi ja politiikan kehittämiseksi. Määrittelytyötä JRC on tehnyt yhteistyössä komission ITS-komitean (C39400) vuonna 2020 perustetun C-ITS-työryhmän (E01941) kanssa, joka myös lopulta hyväksyy uudet C-ITS-turvallisuus- ja varmennepolitiikan versiot ennen niiden julkaisua.

Viimeisin EU:n teknisen tutkimuskeskuksen julkaisema hyväksytty C-ITS-varmennepolitiikan versio (3.0) on julkaistu toukokuussa 2024. Turvallisuuspolitiikasta on julkaistu viimeisin hyväksytty versio (3.0) syyskuussa 2023. Kumpaakin dokumenttia on päivitetty merkittävästi edellisiin, vuoden 2019 C-ITS delegoituun asetusehdotukseen valmisteltuihin versioihin nähden, joskin dokumenttien perusrakenne on pyritty säilyttämään entisenlaisena.

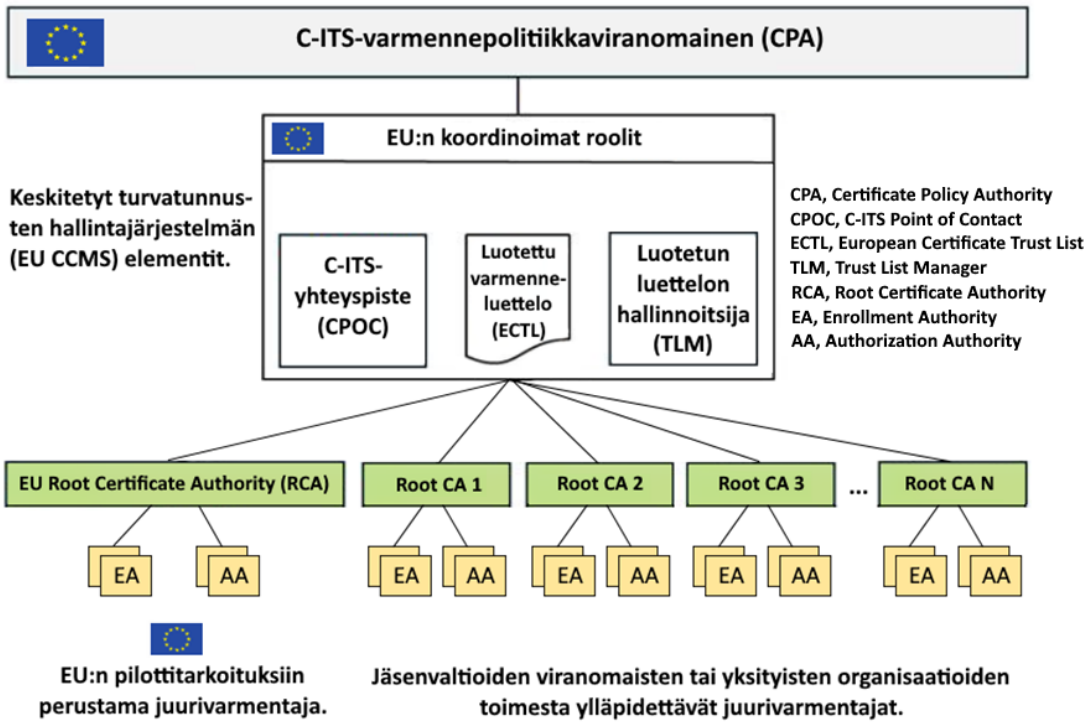
Turvallisuus- ja varmennepolitiikan mukaista C-ITS-palveluiden käyttöönottoa valmistelee tällä hetkellä C-ITS-palveluiden harmonisointia ja käyttöönottoa edistävä EU:n ja kansallisten tieviranomaisten yhteinen yhteistyöfoorumi C-Roads Platform. Turvatunnusten hallintajärjestelmään liittyvistä aiheista yhteistyöfoorumissa vastaa erityisesti WG2-työryhmän (Technical Aspects) tietoturvaratkaisuihin keskittyvä alatyöryhmä (TF1, Security Aspects).

C-ITS-turvallisuus- ja varmennepolitiikan mukaiset EU:n hallinnoimat järjestelmät turvatunnusten jakeluun ja hallintaan ovat olleet valmiita käytännön pilotteja ja demonstraatioita varten jo vuodesta 2020 lähtien (ns. L0-tason tunnusten jakelu ja hallinta). Lopullisiin C-ITS-tuotantoympäristöihin tarkoitettuja turvatunnuksia (ns. L1- ja L2-tasot) on voinut rekisteröidä käyttöön joulukuusta 2024 lähtien. Turvatunnuksia jakelee tällä hetkellä Euroopan komission perustaman ja ATOS:n operoiman EU:n juurivarmennepalvelun lisäksi joitakin yksityisen sektorin toimijoita. L0-tason tunnusten toimintaa on muun muassa testattu Suomessa osana Traficomille toteutettua tutkimus- ja selvitystyötä vuoden 2023 aikana, "Piloting cybersecure and interoperable cellular C-ITS services" (Kynsijärvi et al. 2024).

C-ITS-varmennepolitiikan mukaisesta eurooppalaisen C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) käytön vaatimuksista säädellään vuonna 2023 uudistetussa ITS-direktiivissä. Direktiivi vahvistaa Euroopan komission roolit hallintajärjestelmän toiminnassa sekä sen käytön vaatimukset osana yhteistoiminnallisen, verkottuneen ja automatisoidun liikkumisen ITS-palveluiden toteutusta. (EU 2023/2661 2023)

3.2 C-ITS-varmennepolitiikka

C-ITS-varmennepolitiikka määrittää C-ITS-järjestelmien eurooppalaisen luottamusmallin. Malli perustuu julkisen avaimen menetelmään, ja sitä hyödynnetään osana EU:n C-ITS-turvatunnusten hallintajärjestelmän toimintaa (EU C-ITS Security Credential Management System, EU CCMS). Varmennepolitiikka sitoo kaikkia C-ITS-järjestelmään liittyviä toimijoita. (C-ITS Certificate Policy 2024, 11)



Kuva 1. C-ITS-turvatunnusten hallintajärjestelmän arkkitehtuuri (mukaillen C-ITS Certificate Policy 2024, 15)

Kuvan 1 mukaiset EU:n koordinoimat roolit ja niiden vastuut on kuvattu C-ITS-varmennepolitiikan luvussa 1.3 (C-ITS Certificate Policy 2024, 14–20)

Keskeisin ja ylin varmennepolitiikan mukainen toimija on suoraan Euroopan komission alaisuudessa toimiva **C-ITS-varmennepolitiikkaviranomainen** (CPA). Tämä viranomainen on vastuullinen taho koko varmennepolitiikan sekä PKI-valtuutusten hallinnasta eli valtuuksien myöntämisestä C-ITS-yhteyspisteen (CPOC), luotetun luettelon hallinnoijan (ECTL) sekä juurivarmentajien (RCA) toiminnan harjoittamiseen. C-ITS-varmennepolitiikkaviranomainen tiedottaa luotetun luettelon hallinnoijaa hyväksytyistä/ei-hyväksytyistä juurivarmentajista.

Luotetun luettelon hallinnoitsija (TLM) on yksittäinen C-ITS-varmennepolitiikkaviranomaisen nimittämä taho ja se vastaa luotettujen varmenteiden luettelon (ECTL-luettelo) hallinnasta ja raportoi säännöllisesti omasta toiminnastaan varmennepolitiikkaviranomaiselle. ECTL-luettelo sisältää kaikki toimivat C-ITS-varmennepolitiikkaviranomaisen hyväksymät juurivarmentajat ja juurivarmenteet. Luettelon avulla kaikki PKI-osapuolet voivat luottaa hyväksyttyihin juurivarmentajiin. Luotetun luettelon hallinnoitsija ylläpitää ECTL-luetteloa varmentajista C-ITS-varmennepolitiikkaviranomaisen ilmoitusten perusteella (hyväksytyt/hylätyt juurivarmentajat), vastaanottaa juurivarmenteet C-ITS-yhteyspisteeltä ja välittää säännöllisesti ja oikea-aikaisesti allekirjoitetun ECTL-luettelon C-ITS-yhteyspisteen ja juurivarmentajien käyttöön. C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) akkreditoitu PKI-tarkastaja auditoi luotetun luettelon hallinnoitsijan toiminnan säännöllisesti.

C-ITS-yhteyspiste on yksittäinen C-ITS-varmennepolitiikkaviranomaisen nimittämä taho. C-ITS-yhteyspiste kommunikoi muiden C-ITS-luottamusmallin tahojen (CPA, TLM ja RCA:t) kanssa C-ITS Point of Contact (CPOC) protokollan mukaisella

tavalla, jonka viimeisin versio 3.0 on julkaistu tammikuussa 2024. Protokollan mukaisesti varmennepolitiikkaviranomaisen toteuttaman juurivarmentajan hyväksynnän jälkeen C-ITS-yhteyspiste vastaanottaa juurivarmenteen ja välittää sen ECTL-luetteloon. C-ITS-yhteyspiste vastaa myös hyväksytyn ja allekirjoitetun ECTL-luettelon julkaisusta kaikkien käyttöön.

Uudistetun ITS-direktiivin mukaisesti Euroopan komissio hoitaa kaikkia kolmea yllä kuvattua turvatunnusten hallintajärjestelmän roolia (EU 2023/2661 2023). Näitä rooleja voidaan kuvata C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) **hallinnolliseksi tasoksi** ja keskitettyjen palveluiden toteuttajaksi. Nämä toiminnot tarjoavat EU:n keskitetylle turvatunnusten hallintajärjestelmälle hallinnollisen kehyksen, joka mahdollistaa C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) toiminnan hajauttamisen useille eri juurivarmentajille, joita C-ITS-yksiköiden rekisteröijät (Enrollment Authority, EA) ja valtuuttajat (Authorisation Authority, AA) voivat vapaasti käyttää ristiin, ja C-ITS-yksiköt voivat silti kommunikoida keskenään luotettavasti (”common root of trust”).

C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) keskitettyjen palveluiden alapuolella (kuva 1) toimii hallintajärjestelmän **operatiivinen taso**, jossa joukko C-ITS-varmennepolitiikkaviranomaisen valtuuttamia samanarvoisia juurivarmentajia (Root-CA) yhdessä alivarmentajien (Sub-CA) kanssa muodostavat keskinäisen luottamussuhteen. Varmentajien avulla C-ITS-yksiköt rekisteröidään ja valtuutetaan osaksi eurooppalaista turvallista C-ITS-luottamusmallia. Varmentajien toiminta on määritelty ETSI:n ITS-järjestelmien tietoturvallisuusarkkitehtuureja määrittelevässä standardissa (ETSI TS 102 940 2022, 42–44) sekä C-ITS-varmennepolitiikassa.

Juurivarmentaja (RCA) voi olla kaupallinen toimija, järjestö, kansallinen tai eurooppalainen organisaatio. Juurivarmentaja hakee toimiluvan ETSI TS 102 042 -standardin mukaisesti varmennepolitiikkaviranomaiselta. Toimiluvan hakemisen yhteydessä juurivarmentajan tulee toimittaa organisaation rekisteröimiseen ja tunnistamiseen tarvittavat tiedot, varmentajan digitaalinen sormenjälki (juurivarmenteen SHA-256 tiivistearvo, ”hashvalue”), kryptografiset tiedot juurivarmenteesta (algoritmi, avainten pituudet) sekä kuvata **noudatettavat varmennuskäytännöt** digitaalisten varmenteiden hallintaan liittyen. Kuvattavia varmennuskäytäntöjä ovat esimerkiksi varmenteiden myöntäminen, peruuttaminen ja uusiminen sekä turvatoimet CA-infrastruktuurin suojaamiseksi (Certificate Practise Statement, CPS).

Yllä kuvatut tiedot toimitetaan CPOC-protokollan mukaisesti fyysisesti Euroopan komission tiloihin tekniseen tutkimuskeskukseen (JRC) Italiaan (Ispra). Kun yllä kuvattu hyväksyttämisvaihe on onnistuneesti suoritettu, juurivarmentaja lähettää oman julkisen varmenteen C-ITS-yhteyspisteelle (CPOC), joka lisää sen luotettujen varmenteiden luetteloon (ECTL). C-ITS-yhteyspiste julkaisee julkisesti luotettujen varmenteiden luettelon, jota voi tarkastella C-ITS-yhteyspisteen ylläpitämällä web-sivustolla (https://cpoc.jrc.ec.europa.eu/TLMCertificates.html). Uusin luettelo julkaistaan tyypillisesti kolmen kuukauden välein, ja tarvittaessa useamminkin.

C-ITS-varmennepolitiikan mukaisesti kunkin juurivarmentajan alla toimii kaksi erillistä varmentajaa: C-ITS-yksiköiden **rekisteröijä (EA)** sekä **valtuuttaja (AA)**. C-ITS-yksiköiden rekisteröijä ja valtuuttaja toimivat juurivarmentajan

alivarmentajana, ja ne voivat olla juurivarmentajan tavoin kaupallisia toimijoita, järjestöjä, kansallisia tai eurooppalaisia organisaatioita.

Alivarmentajien toimilupien hakeminen (sertifiointi) on hyvin samanlainen prosessi kuin juurivarmentajankin. Sillä erolla, että kun juurivarmentaja hakee toimiluvan varmennepolitiikkaviranomaiselta, niin alivarmentajat hakevat toimiluvan juurivarmentajalta, jonka alaisuudessa varmennustoiminta tapahtuu. Alivarmentaja lähettää juurivarmentajalle organisaation rekisteröimiseen ja tunnistamiseen tarvittavat tiedot, digitaalisen sormenjäljen sekä kuvauksen varmennuskäytännöistä (CPS).

Yllä kuvattujen toimilupien hakemiseen liittyvien vaatimusten lisäksi kunkin varmentajan (root CA, EA, AA) on toimilupahakemuksen osaksi liitettävä hyväksytty C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) PKI-tarkastajan (PKI auditor) auditointiraportti.

PKI-tarkastaja on C-ITS-turvatunnusten hallintajärjestelmään (EU CCMS) kuuluva toimija, joka auditoi varmentajien (root CA, EA, AA) sekä luotetun luettelon ylläpitäjän (TLM) toiminnan. PKI-tarkastajan rooli ja toimintatavat on kuvattu C-ITS-varmennepolitiikan luvussa 8 (C-ITS Certificate Policy 2024, 80–81).

Varmennetoimijoiden toiminta auditoidaan ensimmäisen kerran, kun toimija hakee toimilupaa sekä säännöllisesti sen jälkeen vähintään kolmen vuoden välein. Auditoitavan toimijan tulee pyytää uusi toiminnan auditointi, mikäli heidän omaan varmennuskäytäntöjen kuvaukseen (CPS) tulee toimintaan vaikuttavia muutoksia. C-ITS-varmennepolitiikkaviranomainen voi pyytää erillisen auditoinnin kaikille toimijoille turvallisuuspolitiikan merkittävissä muutoksissa. Toimintaan tehtävien muutosten ja auditoinnin aikataulu määritetään muutosten kriittisyyden perusteella.

Auditointipyynnön luotetun luettelon hallinnoijalle (TLM) tekee C-ITS-varmennepolitiikkaviranomainen. Juurivarmentajat tekevät omaan toimintaansa liittyvät auditointipyynnöt itse. PKI-tarkastaja keskittyy auditoinnissa varmistamaan erityisesti C-ITS-varmennepolitiikan, toimijan oman varmenteiden hallinnointikuvauksen (CPS) sekä ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmän mukaisen toiminnan. Käytännössä auditoinnin voi suorittaa kuka tahansa Euroopan akkreditointijärjestön jäsenen akkreditoima ja sertifioima riippumaton toimija.

3.3 C-ITS-turvallisuuspolitiikka

C-ITS-turvallisuuspolitiikka yhdessä C-ITS-varmennepolitiikan kanssa muodostaa perustan turvallisten ja yhteen toimivien C-ITS-palveluiden käyttöönotolle Euroopassa.

Edellisessä luvussa esitelty C-ITS-varmennepolitiikka keskittyy C-ITS-yksiköiden välisen viestinnän tietoturvallisuuden varmistamiseen, jossa keskeisessä roolissa on Euroopassa yhteisesti käyttöön otettava julkisen avaimen järjestelmään (PKI) perustuva turvallisuusarkkitehtuuri ja C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS).

C-ITS-turvallisuuspolitiikka keskittyy erityisesti asettamaan puitteet ja perustan tietoturvallisuuden hallinnalle C-ITS-järjestelmien käyttöönottoon ja toimintaan liittyen. Se asettaa tietoturvallisuuden hallintaan liittyviä vaatimuksia erityisesti C-ITS-yksiköitä operoiville tahoille ja muille operointiin liittyville sidosryhmille.

Toinen olennainen osa on C-ITS-yksiköiden käsittelemien tietojen hallinnointiin liittyvät vaatimukset. (C-ITS Security Policy 2023, 2)

Organisaatioiden tietoturvallisuuden hallintaan liittyen turvallisuuspolitiikka vaatii C-ITS-yksiköitä operoivilta organisaatioilta sertifioidun tietoturvallisuuden hallintajärjestelmän. Toimijan roolin mukaan eri toimijoille on asetettu erilaisia hallintajärjestelmävaatimuksia (esim. olennaista liikennepalvelua operoivat tahot, ajoneuvoteollisuus, muu C-ITS-yksiköitä operoiva toimijakenttä). (C-ITS Security Policy 2023, 3)

Toinen olennainen osa C-ITS-turvallisuuspolitiikkaa on C-ITS-yksiköiden käsittelemän tiedon hallinnointiin liittyvät vaatimukset. Tietoa tulee hallinnoida niihin mahdollisesti aiheutuvien tietoturvallisuuden uhkien, mahdollisten tietoturvaloukkausten, näkökulmasta. Uhkia käsitellään perinteisten tiedon turvallisuuteen liittyvien ominaisuuksien osalta, tiedon luottamuksellisuus, eheys ja käytettävyys, sekä näihin liittyvien tietoturvaloukkausten vakavuuden ja vaikutusten näkökulmasta. Huomioon otettavat tietoturvaloukkausten vaikutukset sisältävät liikenneturvallisuuteen, liikenteen sujuvuuteen, taloudellisiin vaikutuksiin ja yksityisyyden suojaan liittyvien näkökulmien tarkastelun. (C-ITS Security Policy 2023, 3–5)

C-ITS-yksiköiden käsittelemien tietojen hallinnointi- ja luokitteluvaatimusten lisäksi C-ITS-turvallisuuspolitiikka asettaa vähimmäisvaatimuksia riskien hallintaan liittyen. Näitä ovat riskien arviointiin liittyvät käytänteet, kuten niiden tunnistaminen, analysointi ja käsittely, joita käsitellään C-ITS-turvallisuuspolitiikan luvussa 2.3. (C-ITS Security Policy 2023, 5–10)

Tarkemmin C-ITS-turvallisuuspolitiikan asettamat vaatimukset ja määritykset C-ITS-yksiköille, niiden operoinnille ja käsittelemälle tiedolle kuvataan seuraavassa luvussa 4.

4 C-ITS-yksiköt ja niiden operointi

C-ITS-yksiköillä tarkoitetaan laitteisto- ja ohjelmistokomponenteista koostuvaa kokonaisuutta, joita käytetään C-ITS-viestien välittämiseen ja vastaanottamiseen. C-ITS-yksiköiden viitearkkitehtuuri määritellään standardissa ETSI EN 302 665. Standardi keskittyy erityisesti määrittelemään erilaisten C-ITS-yksikkötyyppien välisten kommunikaatioiden viitearkkitehtuurin (ITSC, ITS Communications). C-ITS-yksiköt standardi määrittelee neljään eri tyyppiin. C-ITS-yksikkötyypit ovat ajoneuvoyksikkö (vehicle ITS station), tienvarsiyksikkö (roadside ITS station), keskusyksikkö (central ITS station) ja käyttäjän mukana kulkeva henkilökohtainen yksikkö (personal ITS station). C-ITS-yksiköitä hallinnoivista organisaatioista käytetään nimitystä C-ITS-yksikköoperaattori.

C-ITS-yksiköiden yhdenmukaista teknistä toimintaa, kyberturvallisuusvaatimuksia sekä niiden operointiin liittyviä vaatimuksia säännellään useilla eri standardeilla ja EU:n vaatimuksilla. Vaatimukset vaihtelevat myös C-ITS-yksiköiden tyypin perusteella. Tässä luvussa on kuvattu C-ITS-yksiköiden valmistukseen, tietoturvallisuuteen ja niiden operointiin liittyviä vaatimuksia.

C-ITS-turvallisuus- ja varmennepolitiikka määrittelevät eurooppalaisen C-ITS-järjestelmiin liittyvän tietoturvallisuuden hallintamallin (EU CCMS), joka sisältää kolme valmiustasoa (L0, L1, L2) C-ITS-järjestelmien testausvaiheesta (taso L0) kohti täysin vaatimusten mukaista tuotannollista järjestelmää (taso L2). Tässä luvussa C-ITS-yksiköihin sekä niiden operointiin liittyvät vaatimukset ovat lopullisen L2-vaatimustason mukaisia, mikäli ei toisin mainita. Alaluku 4.2.4 kuvaa L2-tason vaatimuksiin liittyviä lievennyksiä, kun toimitaan vielä siirtymätasolla L1.

4.1 C-ITS-yksiköiden valmistus

4.1.1 Tausta

C-ITS-yksiköiden valmistuksella tarkoitetaan fyysisten laitteiden sekä niihin liittyvien ohjelmistojen valmistamista. Osa C-ITS-yksiköistä voi olla vain pelkästään ohjelmistoja (esim. C-ITS-keskusyksiköt). Seuraavissa luvuissa on kuvattu C-ITS-yksiköiden valmistukseen liittyviä ETSI- ja ISO-standardeihin, EU-direktiiveihin sekä C-Roads-spesifikaatioihin perustuvia vaatimuksia.

Valmistukseen liittyvät vaatimukset tulee huomioida luonnollisesti osana C-ITS-yksiköiden valmistusta (esim. C-ITS-keskusyksikön ohjelmistokehitys), mutta myös osana niiden hankintaa, jotta hankinnan yhteydessä osataan vaatia oikeat C-ITS-yksiköiden hyväksynnät ja sertifikaatit.

4.1.2 ETSI-standardit ja yhteentoimivuustestit

C-ITS-yksiköiden (mukaan lukien C-ITS-keskusyksiköt) sekä PKI-avainten toimittajien järjestelmien tulee toimia standardien ETSI TS 102 941 sekä ETSI TS 103 097 mukaisesti (uusimmat versiot v.2.2.1 ja v.2.1.1). Standardit määrittelevät C-ITS-järjestelmien välisen viestinnän luottamuksen ja yksityisyyden hallinnan sekä viestien turvalliset tietorakenteet.

C-ITS-yksiköiden standardienmukaisuutta ja keskinäistä yhteentoimivuutta pyritään varmistamaan standardissa ETSI TS 103 600 määritellyillä yhteentoimivuutta koskevilla testeillä. ETSI-standardointijärjestö järjestää C-ITS-yksiköiden valmistajille sekä juurivarmennuspalveluiden toimittajille yhteentoimivuutta

koskevia testaustilaisuuksia vuosittain (ns. ”ETSI Plugtest™”). Noin viikon mittaisissa testeissä toteutetaan laitteiden väliseen kommunikaatioon liittyviä testitapauksia, joilla pyritään varmistamaan osallistujien toteuttamien ratkaisujen keskinäinen yhteentoimivuus.

ETSI-järjestön CTI-yksikkö (Centre for Testing and Interoperability) järjestää vuosittain yllä kuvattuja yhteentoimivuutta koskevia testaustilaisuuksia, joihin kaikki halukkaat laite- ja ohjelmistovalmistajat sekä muut organisaatiot voivat vapaasti osallistua testaamaan tuotteidensa yhteentoimivuutta eri valmistajien välillä. Kyseinen C-ITS-yksiköiden testausprosessi ei siis (ainakaan tällä hetkellä) ole Euroopan komission virallinen vaatimus C-ITS-yksiköiden valmistukseen tai käyttöönottoon liittyen, vaan pikemminkin prosessi, jonka avulla niiden yhteentoimivuutta voidaan laajasti testata muiden laitevalmistajien kanssa yhteisesti. Testeihin osallistuminen vaatii tyypillisesti salassapitosopimuksen allekirjoittamista (muiden laitevalmistajien tuotteisiin ja niiden toimintaan liittyvä salassapitovelvoite) ja osallistumisesta saa todistuksen. ETSI-järjestön tekniset komiteat käyttävät kyseisiä tapahtumia myös standardien kehittämiseksi laite- ja ohjelmistovalmistajilta saadun palautteen avulla.

4.1.3 ISO 15408 – Common Criteria

EU C-ITS-turvallisuuspolitiikka määrittelee, että C-ITS-yksiköiden tietoturvallisuuden taso on arvioitava standardin ISO/IEC 15408 (ns. ”Common Criteria”) mukaisesti. Standardi koostuu viidestä osasta ja sen viimeisin versio (neljäs editio) on julkaistu elokuussa 2022.

ISO 15408 on kehitetty erityisesti IT-tuotteiden tietoturvallisuuden tason arviointiin ja varmistamaan, että tuotteen tietoturvallisuuden taso täyttää asiakkaiden (riskin omistajan) tarpeet. Tuotteet voivat olla laajasti erilaisia laitteita, laiteohjelmistoja (firmware) tai ohjelmistoja. (ISO/IEC 15408-1 2022)

C-ITS-yksikön tietoturvallisuuden tason sertifiointiprosessi on kaksivaiheinen:

(1) **C-ITS-yksikön turvaprofiilin (PP, Protection Profile) määrittely ja sertifiointi.** Ensimmäisessä vaiheessa tulee määritellä C-ITS-yksikön tietoturvallisuustason arvioinnin laajuus (Target Of Evaluation, TOE). Tämä toteutetaan niin sanotun turvaprofiilin avulla. Turvaprofiili sekä siihen liittyvät asiakirjat sertifioidaan hyväksytyn auditointiorganisaation toimesta. (C-ITS Security Policy 2023, 9)

    Arvioinnin kohteen ja turvaprofiilin määrittely on oleellista, koska standardi on joustava eikä lähtökohtaisesti ota kantaa, tehdäänkö tietoturvallisuuden arviointi kokonaiseen tuotteeseen tai vain osaan siitä.

(2) **C-ITS-yksikön tietoturvallisuuden tason sertifiointi** turvaprofiilin määrittelemässä laajuudessa**.** C-ITS-turvallisuuspolitiikka määrittelee (kohta 27), että C-ITS-yksikön tietoturvallisuuden taso tulee arvioida ja sertifioida ISO 15408 standardin määrittelemien tietoturvallisuuden EAL-tasoluokitusten (Evaluation Assurance Level) mukaisesti (C-ITS Security Policy 2023, 9). C-ITS-varmennepolitiikka määrittää (kohta 323), että tietoturvallisuuden tason arvioinnin tuloksena tulee saavuttaa kyseisen tasoluokituksen mukainen tietoturvavaatimusten toteutumistaso EAL4 (C-ITS Certificate Policy 2024, 74). Standardi sisältää tietoturvatasot EAL1–EAL7.

ISO 15408 -standardissa olevan kuvauksen mukaisesti EAL4-taso vaatii hyvät kehityskäytännöt, jotka ovat tiukkoja mutta eivät vaadi merkittäviä erityisosaamisia, -taitoja tai -resursseja. Taso on sovellettavissa tilanteissa, joissa kehittäjiltä vaaditaan kohtuullista tai korkeaa tietoturvallisuuden hallintaan liittyvää osaamistasoa sekä itsenäistä kykyä turvallisuuden varmistamisessa tavanomaisissa kaupallisten ohjelmistojen valmistus- ja kehityskohteissa. (ISO/IEC 15408-1 2022)

Turvaprofiilien määrittelystä eli tietoturvallisuuden tason määrittelyn laajuudesta käytännössä vastaa "riskin omistaja". Euroopassa C-ITS-järjestelmän tietoturvallisuudesta vastaa C-ITS-varmennepolitiikkaviranomainen (CPA) eli Euroopan komissio. C-ITS-varmennepolitiikkaviranomainen luo valmiita turvaprofiileja erilaisille C-ITS-yksikkötyypeille varmistaakseen yksiköiden tietoturvallisuuden tason arvioinnin riittävän laajuuden. C-ITS-yksiköiden valmistajat ovat velvoitettuja käyttämään näitä turvaprofiileja tietoturvallisuuden tason arvioinnissa. Hyväksytyt C-ITS-yksiköiden turvaprofiilit julkaistaan samassa paikassa turvallisuus- ja varmennepolitiikkadokumenttien kanssa.

C-ITS-varmennepolitiikkaviranomainen on luonut valmiit turvaprofiilit C-ITS-tienvarsi- ja ajoneuvoyksiköille. Näiden yksiköiden osalta turvaprofiili määrittelee, että tietoturvallisuuden tason arviointi tulee kohdistaa erityisesti C-ITS-yksikön salausmoduuliin (Hardware Secure Module, HSM), joka suojaa laitteeseen tallennettuja PKI-avaimia sekä C-ITS-yksikön laiteohjelmistoon (C-ITS Certificate Policy 2024, 74).

C-ITS-varmennepolitiikan mukaisesti (kohta 25) uusien C-ITS-yksiköiden kehittämisen yhteydessä C-ITS-varmennepolitiikkaviranomaiselle syntyy tarve määritellä uusiin C-ITS-yksiköihin soveltuvia turvaprofiileja. Mikäli käyttöönotettavaan C-ITS-yksikköön ei ole vielä toteutettu valmista turvaprofiilia, C-ITS-yksikön valmistaja voi itse määritellä turvaprofiilin, ja C-ITS-varmennepolitiikkaviranomaisen toteuttaman turvaprofiilin hyväksynnän jälkeen C-ITS-yksikön turvallisuustaso voidaan arvioida. Arvioinnin vaatimustasona tässä tapauksessa on alempi tietoturvataso EAL2. (C-ITS Security Policy 2023, 9)

Yllä oleva on hyvä huomioida osana mahdollista suomalaista C-ITS-järjestelmän käyttöönottoa, joka mahdollisesti perustuessaan pitkän kantaman tiedonsiirtoon sisältäisi käytännössä vain ohjelmistopohjaisia C-ITS-keskusyksiköitä, joille varmennepolitiikkaviranomainen ei ole määritellyt keskusyksiköiden tietoturvatason arviointiin vaadittavaa turvaprofiilia.

Mikäli Suomessa valmistetulle C-ITS-keskusyksikölle halutaan saada ISO 15408 –standardin mukainen tietoturvatason arviointi, tietoturvatason voi arvioida FINASin (Finnish Accreditation Services) hyväksymä suomalainen arviointiyksikkö. Suomessa ei ole kuitenkaan tunnistettu kyseisiin auditointeihin FINAS-hyväksyttyjä toimijoita älykkään liikkumisen tai ylipäätään liikenteen pätevyysalueella. Tässä tapauksessa sertifioinnin voi toteuttaa SOG-IS-sopimuksen (Senior Officials Group on Information Systems Security) piirissä tunnistettu eurooppalainen arviointiyksikkö, jonka tekemä arviointi on MRA-sopimuksen (Mutual Recognition Agreement) vastavuoroisen tunnustamisen periaatteiden mukaisesti voimassa koko Euroopassa.

4.1.4 EU-radiolaitedirektiivi

Radioteknologioita hyödyntäviin C-ITS-yksiköihin (ajoneuvoyksiköt, tienvarsiyksiköt ja henkilökohtaiset C-ITS-yksiköt) sovelletaan yllä kuvattujen tuotteiden tietoturvallisuuden hallintaan liittyvien vaatimusten lisäksi myös EU:n radiolaitedirektiivin delegoitua asetusta EU/2022/30. Delegoitu asetus koskee erityisesti radiolaitteita, jotka voivat viestiä Internet-verkon kautta joko suoraan tai toisen laitteen välityksellä (”Internet-verkkoon liitettävät radiolaitteet”). Asetus sisältää vaatimuksia mm. radioverkon resurssien käyttöön, verkolle aiheutuviin häiriöihin ja henkilötietojen suojaamiseen liittyen (Kotilainen et al. 2023). Uuden radiolaitedirektiivin soveltamisajankohtaa on siirretty alkuperäisestä (1.8.2024) vuodella eteenpäin, jotta tietoturvavaatimusten teknisten standardien valmisteluun saadaan enemmän aikaa.

4.2 C-ITS-yksiköiden operointi

C-ITS-yksiköiden operoinnilla tarkoitetaan C-ITS-yksiköiden vastuullista hallinnoimista. C-ITS-yksikköoperaattori vastaa C-ITS-yksiköiden hankinnasta, liittämisestä osaksi C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS), asennuksesta, vianselvitystoiminnasta sekä C-ITS-yksiköiden ja niiden käsittelemän tiedon tietoturvallisuudesta.

C-ITS-turvallisuuspolitiikka keskittyy erityisesti C-ITS-yksiköihin liittyviin vaatimuksiin niiden operoinnin lähtökohdista.

4.2.1 C-ITS-yksikköoperaattori

Taulukossa 1 on kuvattu mahdolliset C-ITS-yksiköiden operoijat eri standardin ETSI EN 302 665 mukaisissa C-ITS-yksikkötyypeissä.

Taulukko 1. C-ITS-yksiköiden operaattorit yksikkötyyppien perusteella

C-ITS-yksikkötyyppi	Mahdolliset operoijat
Ajoneuvoyksikkö (Vehicle ITS-station)	Ajoneuvovalmistaja (ajoneuvoihin integroidut yksiköt), viranomainen (esim. hälytysajoneuvot), joukkoliikennetoimijat sekä yksityiset palveluntarjoajat, kuten hinauspalveluiden tarjoajat, kiireellistä sairaankuljetusta tarjoavat yritykset, tien talvikunnossapitoa suorittavat urakoitsijat tai ei-virkasuhteessa toimiva palokunta.
Tienvarsiyksikkö (Roadside ITS-station)	Tienpitäjä (valtio/Väylävirasto, kunta) tai muu katuverkon toimija (kuten kunnossapitourakoitsija, jonka kalusto voisi olla varustettu lyhyen kantaman C-ITS-tienvarsiyksiköillä).
Keskusyksikkö (Central ITS-station)	Fintraffic (valtion hallinnoimat tieosuudet), kunta (kuntien tie- ja katuverkot, esim. kaupunkikohtaisen C-ITS-keskusyksikön operointi), ajoneuvovalmistaja (ajoneuvojen sisälle integroitavien C-ITS-ajoneuvoyksiköiden keskusjärjestelmä pitkän kantaman tiedonsiirtoon perustuvassa ratkaisussa), joukkoliikenneoperoija, muu viranomainen tai yksityinen kaupallinen toimija (esim. yksityinen mobiiliapplikaatioiden avulla C-ITS-palveluita tarjoava C-ITS-palveluntarjoaja).
Henkilökohtainen yksikkö (Personal ITS-station)	Yksikön valmistaja (työryhmän tiedossa ei ole, että henkilökohtaisia C-ITS-yksiköitä olisi vielä valmistettu).

4.2.2 Tietoturvallisuuden hallintajärjestelmävaatimukset

Tässä luvussa esitetyt tietoturvallisuuden hallintajärjestelmävaatimukset on kuvattu C-ITS-turvallisuuspolitiikan luvussa 2.1 (C-ITS Security Policy 2023, 3).

C-ITS-turvallisuuspolitiikka määrittelee, että C-ITS-yksikköoperaattorilla tulee olla standardin ISO/IEC 27001 mukainen sertifioitu tietoturvallisuuden hallintajärjestelmä (Information Security Management System, ISMS). Turvallisuuspolitiikassa vaaditaan, että hallintajärjestelmän tulee kattaa sen normaalien vaatimusten lisäksi kyseisen toimijan operoimien C-ITS-yksiköiden sekä niiden käsittelemän tiedon turvallisuuden hallinta, kuten tiedon luokittelu ja tietoa käsittelevät taustajärjestelmät.

Vaihtoehtoisesti ajoneuvoihin integroitujen C-ITS-ajoneuvoyksiköiden operointiin liittyen C-ITS-yksikköoperaattori (tyypillisesti ajoneuvovalmistaja) voi olla sertifioitu ajoneuvoteollisuuden kyberturvallisuuden hallintaan tarkoitetun UN Requlation No. 155 säädöksen (UN R155)[1] mukaisella kyberturvallisuuden hallintajärjestelmällä (Cyber Security Management System, CSMS). Niiltä osin, kun edellä mainittu CSMS-järjestelmä ei kata C-ITS-yksikköoperaattorin toimintaa esimerkiksi tiedonvaihdon rajapintojen tai tiedon käsittelyn osalta, tulee näiden osuuksien tietoturvallisuus turvata standardin ISO 27001 mukaisella sertifioidulla tietoturvallisuuden hallintajärjestelmällä.

C-ITS-yksikköoperaattorit, jotka tuottavat olennaista liikennepalvelua NIS- tai NIS2-kyberturvallisuusdirektiivien[2] mukaisesti, voivat soveltaa tietoturvallisuuden hallintaan kyseisten direktiivien vaatimuksia. Liikennepalvelua tuottavalle toimijalle riittää kyseisissä direktiiveissä esitettyjen vaatimusten kattava vaatimustenmukaisuuden arviointi, jonka on suorittanut kansallisen viranomaisen tehtävään akkreditoima toimija.

Yllä kuvattujen tietoturvallisuuden hallintajärjestelmien sertifiointivaatimusten lisäksi C-ITS-turvallisuuspolitiikka velvoittaa C-ITS-yksikköoperaattoreita huolehtimaan, että sertifioitu turvallisuuden hallintajärjestelmä on yhdenmukainen C-ITS-turvallisuuspolitiikan kanssa. Erityisesti tämä koskee C-ITS-yksiköiden käsittelemien tietojen hallinnointiin liittyviä vaatimuksia, jotka on kuvattu tämän dokumentin luvussa 4.2.3.

C-ITS-turvallisuuspolitiikan luku 2.1 määrittää myös, että yksikköoperaattoreiden tulee tunnistaa C-ITS-järjestelmiin ja niiden toimintaan sidonnaiset säädökset, kuten yhteistoiminnallisten liikennejärjestelmien eurooppalainen strategia (EU C/2016/766 2016) sekä EU:n yleinen tietosuoja-asetus (GDPR)[3]. Yksikköoperaattoreiden tulee myös tunnistaa omaan toimintaansa liittyvät sidosryhmät, jotka ovat olennainen osa tietoturvallisuuden hallintajärjestelmää ja sen asettamia vaatimuksia.

---

[1] Vuonna 2021 (01/2021) voimaan tulleen UN R155 -säädöksen (osa autoteollisuuden niin sanottua ”e-säännöstöä”) tavoite on kehittää ajoneuvojen kyberturvallisuutta, ja se on osa laajempaa pyrkimystä parantaa ajoneuvojen luotettavuutta sekä turvallisuutta digitaalisten uhkien aikakaudella (UN Regulation No. 155, 2021). UN R155 -säädöksen on valmistellut UNECE (The United Nations Economic Commission for Europa) eli Euroopan alueen talouskomissio.

[2] NIS2-direktiivi (Network and Information Security, EU 2022/2557 2022) on eurooppalaisen kyberturvallisuusdirektiivin toinen versio, joka astui voimaan lokakuussa 2024. Se määrittelee eurooppalaiset kriittiset toiminta-alueet, joihin sen vaatimukset kohdistuvat (liikenneala on yksi niistä). Se määrittelee toimialalla toimiville organisaatioille vaatimukset niiden kyberturvallisuuden hallinnasta. Tyypillisesti nämä vaatimukset ovat suurimmalta osin helpoin täyttää sertifioimalla standardin ISO/IEC 27001 mukainen tietoturvallisuuden hallintajärjestelmä.

[3] GDPR (General Data Protection Regulation) on Euroopan unionin asetus, jonka avulla pyritään yhtenäistämään tietosuojaa koskeva lainsäädäntö Euroopan alueella. Asetusta alettiin soveltamaan 25. toukokuuta 2018. (EU 2016/679, 2016)

4.2.3 C-ITS-tiedon hallinnointi

C-ITS-turvallisuuspolitiikka määrittelee C-ITS-yksiköiden toimintaan liittyvät tiedon hallinnoinnin vaatimukset, jotka tulee olla yhdenmukaisia yksikköoperaattorin tietoturvallisuuden hallintajärjestelmän kanssa. Tiedon hallintaan liittyvät vaatimukset ovat (1) tietojen ja niihin liittyvien riskien luokittelu, (2) riskien arviointi luokitteluperusteiden mukaisesti ja (3) riskien käsittelyn periaatteet.

Tietojen ja niihin liittyvien riskien luokittelu

C-ITS-turvallisuuspolitiikka määrittää luvussa 2.2, että yksikköoperaattorin tulee arvioida ja luokitella C-ITS-yksiköiden käsittelemään tietoon kohdistuvia uhkia tiedon turvallisuuteen liittyvien ominaisuuksien (luottamuksellisuus, eheys, käytettävyys) sekä tietoturvaloukkausten vakavuuden ja vaikutusten näkökulmista.

Taulukko 2. Tietoturvaloukkausten arviointi (C-ITS Security Policy 2023, 4)

	Mahdollinen vaikutus		
Turvallisuustavoite	PIENI	KOHTALAINEN	SUURI
Luottamuksellisuus Noudatetaan sovittuja sääntöjä tietojen käytön ja luovutuksen suhteen sekä keinot yksityisyyden suojan ja luottamuksellisten tietojen suojaamiseksi.	Tietojen luvattoman luovuttamisen haittavaikutus on **rajallinen** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.	Tietojen luvattoman luovuttamisen haittavaikutus on **vakava** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.	Tietojen luvattoman luovuttamisen haittavaikutus on **erittäin vakava tai katastrofaalinen** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.
Eheys Suojaudutaan tietojen luvattomalta muuttamiselta ja tuhoamiselta sisältäen tiedon kiistämättömyyden ja aitouden varmistamisen.	Tietojen luvattoman muuttamisen tai tuhoamisen haittavaikutus on **rajallinen** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.	Tietojen luvattoman muuttamisen tai tuhoamisen haittavaikutus on **vakava** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.	Tietojen luvattoman muuttamisen tai tuhoamisen haittavaikutus on **erittäin vakava tai katastrofaalinen** organisaation toimintoihin, omaisuuteen tai yksittäisiin henkilöihin.
Saatavuus Varmistetaan tiedon oikea-aikainen ja luotettava saatavuus ja käyttö.	Tietojen saatavuuteen tai käyttöön kohdistuvien häiriöiden haittavaikutus on **rajallinen** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.	Tietojen saatavuuteen tai käyttöön kohdistuvien häiriöiden haittavaikutus on **vakava** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.	Tietojen saatavuuteen tai käyttöön kohdistuvien häiriöiden haittavaikutus on **erittäin vakava tai katastrofaalinen** organisaation toimintoihin ja omaisuuteen tai yksittäisiin henkilöihin.

Turvallisuuspolitiikka määrittelee, että C-ITS-palveluiden toteutuksissa käytettyjen viestien (CAM, DENM, IVIM, MAPEM, SPATEM, SSEM, SREM) luottamuksellisuuteen, eheyteen tai käytettävyyteen liittyvät tietoturvaloukkaukset aiheuttavat lähtökohtaisesti joko yllä kuvatun taulukon 2 mukaisia pieniä tai kohtalaisia organisaation toimintoihin, omaisuuteen tai yksittäisiin henkilöihin kohdistuvia vaikutuksia.

C-ITS-yksikköoperaattorin on arvioitava tietoturvaloukkausten C-ITS-sidosryhmille aiheuttamia vahinkoja ja kustannuksia seuraavien vaikutusalueiden näkökulmasta:

- **Turvallisuus**: vaikutus aiheuttaa välittömän loukkaantumisriskin tienkäyttäjille tai C-ITS-sidosryhmille.
- **Toiminnalliset vaikutukset**: vaikutus heikentää merkittävästi liikenteen sujuvuutta tai aiheuttaa muita yhteiskunnallisia vaikutuksia, kuten ympäristöhaittoja tai järjestäytynyttä rikollisuutta.
- **Taloudelliset vaikutukset**: vaikutus aiheuttaa suoria tai välillisiä kustannuksia yhdelle tai useammalle C-ITS-sidosryhmälle.
- **Yksityisyys**: EU:n yleisen tietosuoja-asetuksen (GDPR) rikkomisesta aiheutuu sekä oikeudellisia että taloudellisia seurauksia.

Riskien arviointi

C-ITS-turvallisuuspolitiikka velvoittaa C-ITS-yksikköoperaattoreita monipuolisesti arvioimaan C-ITS-tietojen käsittelyyn liittyviä riskejä (C-ITS Security Policy 2023, 5–7). Se velvoittaa yksikköoperaattoria tunnistamaan ja arvioimaan C-ITS-palveluiden yhteydessä käsiteltäviin tietoihin kohdistuvia riskejä määräajoin. Riskien arviointi tulee dokumentoida ja sen tulee sisältää seuraavat riskien arviointiin liittyvät näkökulmat standardien ISO/IEC 27005 tai ISO/SAE 21434 ohjeiden ja vaatimusten mukaisesti.

- **Riskien arvioinnin kohde** sisältäen C-ITS-järjestelmän kuvauksen (tarkoitus, rajaus, järjestelmän käsittelemä tieto).
- Mahdollisten eri tasoisten **tietoturvaloukkausten vaikutukset** edellisessä luvussa kuvattujen vaikutusalueiden näkökulmasta.
- **Riskien tunnistaminen**, jonka lähtökohtana toimii suojattavien tietojen tunnistaminen ja määrittely (C-ITS-viestit ja muut palveluiden toteutuksessa tarvittavat tiedot) sekä näihin liittyvien mahdollisten uhkien ja haavoittuvuuksien tunnistaminen. Uhkia ja haavoittuvuuksia tulee tarkentaa tapausskenaarioiden avulla, joissa tunnistetaan uhkien lähteet ja tietoturvaloukkausten seuraukset.
- **Riskien analysoinnissa** käytetään hyväksi riskien arviointiin liittyvää tietoturvaloukkausten vaikutusten laajuutta (pieni, kohtalainen, suuri) sekä tapausskenaarioiden avulla tunnistettua tapahtuman todennäköisyyttä (epätodennäköinen, mahdollinen, todennäköinen). Lopullista riskitasoa arvioidaan näiden kahden muuttujan tulona taulukon 3 mukaisesti.

Taulukko 3. Mahdollisten tietoturvaloukkausten todennäköisyyden ja vaikutuksen tulona kuvattu riskitasojen määrittäminen (C-ITS Security Policy 2023, 6)

Riskitasot vaikutuksen ja todennäköisyyden tulon perusteella		Todennäköisyys		
		Epätodennäköinen (1)	Mahdollinen (2)	Todennäköinen (3)
Vaikutus	Pieni (1)	Alhainen (1)	Alhainen (2)	Kohtalainen (3)
	Kohtalainen (2)	Alhainen (2)	Kohtalainen (4)	Korkea (6)
	Suuri (3)	Kohtalainen (3)	Korkea (6)	Korkea (9)

Tässä luvussa kuvatun riskien arvioinnin periaatteiden ja taulukon 3 mukaisia C-ITS-palveluun kohdistuvia kohtalaisen tai korkean riskitason riskejä tulee käsitellä seuraavan luvun mukaisesti (riskien käsittely).

Riskien käsittely

Tässä luvussa kuvataan riskien käsittelyyn liittyvät C-ITS-turvallisuuspolitiikan mukaiset vaatimukset. Käsittelyyn liittyvät erilaiset lähestymistavat sekä riskien hallintaan liittyvät toimet, joilla pyritään varmistamaan C-ITS-palveluiden käsittelemän tiedon luottamuksellisuutta, eheyttä ja käytettävyyttä.

Tunnistetut riskit tulee käsitellä aina jollain alla kuvatulla tavalla ja niiden käsittelytoimenpiteet on dokumentoitava kulloinkin sovellettavan standardin mukaisesti.

- Riskitason alentaminen C-ITS-turvallisuuspolitiikan luvuissa 2.4.2 ja 2.4.3 kuvatuilla riskien kontrollointiin keskittyvillä keinoilla (C-ITS Security Policy 2023, 7–9).
- Riskitason säilyttäminen (mikäli riskitaso on hyväksyttävä eli alhainen).
- Riskin välttäminen.
- Riskin jakaminen tai siirtäminen. Tätä ei saa tehdä kuitenkaan niin, että toimenpide aiheuttaa toiselle C-ITS-toteutuksen toimijalle hyväksymättömän riskitason riskin (kohtalainen, korkea).

Riskienhallinta ja siihen liittyvät vaatimukset ovat osa riskien käsittelyä. C-ITS-turvallisuuspolitiikka määrittelee riskienhallintaan liittyviä keinoja pääasiassa perustuen C-ITS-yksiköiden valmistukseen, niiden väliseen viestintään ja niiden toimintaan osana C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS). Keinot perustuvat pääasiassa C-ITS-turvallisuus- ja varmennepolitiikoissa mainittuihin vaatimuksiin liittyen toiminnassa sovellettaviin standardeihin.

Osa yllä mainituista riskienhallinnan keinoista on jo esitelty tässä selvitystyössä. Alla on kuvattu koostetusti kaikki C-ITS-turvallisuuspolitiikan tietoturvaloukkausten kontrollointiin liittyvät keinot.

- C-ITS-yksiköiden riskienhallintaan tulee soveltaa ISO/IEC 27001 tai UN R155 (liite 5) standardeissa kuvattuja keinoja.
- Liikkuvan C-ITS-yksikön viestinnän yksityisyyden suojaamiseksi (luottamuksellisuus) lähettäjän tulee käyttää viestinnässä vaihtuvia valtuutuslippuja (AT, Authorization Ticket). Valtuutuslipulla vahvistetaan viestijän oikeus osallistua tiettyjen C-ITS-palveluiden (viestityypit) viestintään. Ne toimivat lyhytaikaisina varmenteina mahdollistaen viestinnän ilman, että laitteen tai ajoneuvon oikea tai pseudonymisoitu identiteetti paljastuu.
- Kiinteiden ja liikkuvien C-ITS-yksiköiden lähettämän ja vastaanottaman tiedon eheys varmistetaan standardin ETSI TS 103 097 mukaisella viestien allekirjoittamisella. Toimiessaan osana IP-verkkoa (Internet Protocol), C-ITS-yksiköt voivat käyttää myös ISO 21777 -standardiin pohjautuvaan tulevaan ETSI ITS -standardiin perustuvia varmenteita.
- Saatavuuteen liittyen määritellään, että liikennevalon tilatietoa kysyvän (liikkuvan yksikön) SREM-viestiin (Signal Request Extended Message) on vastaanottajan vastattava signaalin tilatiedon sisältävällä SSEM-viestillä (Signal request Status Extended Message).
- C-ITS-turvallisuuspolitiikka tuo esiin seuraavia keinoja C-ITS-yksiköiden käsittelemien tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien tietoturvariskien kontrollointiin:
    - C-ITS-yksiköiden valmistamiseen liittyvät standardin ISO 15408 (Common Criteria) mukaiset vaatimukset. Nämä vaatimukset on kuvattu tarkemmin tämän selvityksen luvussa 4.1.3.
    - C-ITS-yksiköiden tulee olla yhteentoimivia varmennepolitiikan vaatimusten kanssa toimiessaan osana C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS).
    - C-ITS-yksiköiden tietoturvaloukkausten hallittu käsittely. NIS2-direktiivin määräysten lisäksi yksiköiden on tarjottava lokitietoa tietoturvaloukkaukseen liittyvistä tapahtumista jälkikäteen tehtävää analysointia varten.
    - C-ITS-yksikköoperaattorilla tulee olla sertifioitu standardin ISO 27001 mukainen tietoturvallisuuden hallintajärjestelmä, ellei kyseessä ole tienpitäjä, jolle riittää NIS1- ja NIS2-direktiiveissä esitettyjen vaatimusten kattava vaatimustenmukaisuuden arviointi. Nämä vaatimukset on kuvattu tarkemmin tämän selvityksen luvussa 4.2.2.

4.2.4 Tietoturvatasoon L1 liittyvät lievennykset

C-ITS-palveluiden käyttöönoton tukemiseksi C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) määrittelee kolme tasoa (L0-L2), jotka tarjoavat kehityspolun testivaiheesta täysin C-ITS-varmenne- ja turvallisuuspolitiikkojen vaatimusten mukaiseen toteutukseen.

Tässä luvussa kuvataan karkeasti kolmen tason vaikutukset erityisesti C-ITS-yksiköille sekä niiden operaattoreille. Luku perustuu C-ITS Point of Contact Protocol määrittelydokumentin liitteeseen 8 (CPOC Protocol 2024, 89–103)

L0-taso on tarkoitettu C-ITS-yksiköiden testaamiseen ja osaamisen kehittämiseen kohti C-ITS-turvastandardien ja teknisten vaatimusten vaatimustenmukaisuutta. L1 on väliaikainen ympäristö eli C-ITS-palveluiden siirtymävaiheena kohti varsinaista L2-tason tuotantoympäristöä. On hyvä huomioida, että C-ITS-yksiköiden testaaminen sinänsä ei vaadi niiden L0-rekisteröintiä. L0-ympäristö on tarkoitettu C-ITS-yksiköiden yhteentoimivuustesteihin osana C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS). L0-ympäristöä tarjotaan ajallisesti rajoitettuihin testausjaksoihin (esim. C-Roads pilotoinnit), jotka sovitaan PKI-osallistujien rekisteröinnin yhteydessä.

L1- ja L2-tasot tarjoavat tuotantoympäristöt, jossa L1 on tarkoitettu C-ITS-yksiköille, jotka eivät vielä täytä varmenne- ja turvallisuuspolitiikan vaatimuksia. L1-tason määrittelyyn liittyy myös ”L1 Legacy” -taso. Tällä tarkoitetaan vaihetta, jossa L1-tason siirtymävaiheen palvelut on jo lopetettu, mutta siirtymävaiheen aikana käyttöönotetut yksiköt jatkavat toimintaansa osana L2-tason ympäristöä.

L1-taso on tarkoitettu ensisijaisten C-ITS-palveluiden käyttöönoton tukemiseksi siirtymävaiheen aikana. C-Roadsin mukaan siirtymävaihe on ajoitettu vuoden 2025 loppuun saakka (CPOC Protocol 2024, 92). Siirtymävaiheen aikana on kaksi vuotta aikaa tuotteen kehittämiseen ja sertifioimiseen, minkä jälkeen L1-tason tuotannossa olevat C-ITS-palvelut tulisi siirtää L2-tasolle. Aikataulu tuskin tulee pitämään, sillä C-ITS-yhteyspisteellä on voinut L1- ja L2-tason varmenteita rekisteröidä käyttöön vasta joulukuusta 2024 lähtien.

L1-tason tavoitteena on toimia siirtymävaiheena pilotointiin tarkoitetun L0-tason ja pysyvän tuotantovaiheen tasoksi tarkoitetun L2-tason välillä. C-ITS-palveluissa käytettäviin C-ITS-yksiköihin ja niiden operointiin liittyen on määritelty L1-tason vaatimusten lievennyksiä suhteessa L2-tason palveluihin. Tämän kahdeksankohtaisen listan lievennykset 1–4 koskevat C-ITS-yksikköön liittyviä turvallisuus- ja toiminnallisuusvaatimuksia, kohdat 5–6 koskevat C-ITS-yksikköoperaattorien tietoturvallisuusjärjestelmään liittyviä lievennyksiä ja loput lievennykset (7–8) liittyvät PKI-toimijoihin. Alla olevassa taulukossa 4 on lyhyesti kuvattu kunkin lievennyksen sisältö.

Taulukko 4. CPOC-dokumentin liitteen 8 määrittelemät L1-tason lievennykset. Taulukkoon on L1-tason lievennys sarakkeeseen lisätty L1-lievennyksen perään myös L2-tason vaatimus (CPOC Protocol 2024, 94–96)

Id	Kohde	Viite	L1-tason lievennys	Siirtymävaiheen jälkeen
1	C-ITS-yksikkö, CC-sertifiointi	Turvallisuuspolitiikka (25)	Yksikön arviointi SOG-IS tunnustetussa laboratoriossa. Suojaus perusuhkia vastaan tason EAL1 vaatimusten mukaisesti. Lisäys: L2-tavoitetaso on Common Criterian mukainen tietoturvallisuuden taso EAL4.	Sama poikkeus sallitaan ennen siirtymävaiheen loppua käyttöönotetuille yksiköille.
2a	C-ITS-yksikkö, tietoturvayksikkö	Varmennepolitiikka (324)	Valmistajalla ISO 27001 sertifiointi. Laitealustan saavutettava (tulevaisuudessa) Common Criteria EAL4-taso (laitteisto + firmware). Lisäys: Ei tarvitse olla vielä L1-tasolla EAL4-taso, kts. alla oleva vaatimuksen toinen osa (2b).	Sama poikkeus sallitaan ennen siirtymävaiheen loppua käyttöönotetuille yksiköille.
2b	C-ITS-yksikkö, tietoturvayksikkö	Varmennepolitiikka (324)	SOG-IS MRA-akkreditoitu laboratoriosta lähetettävä 6 kk välein edistymisraportteja, jotka CPA arvioi säilyttääkseen L1-rekisteröinnin.	Sama poikkeus sallitaan.
3	C-ITS-yksikkö, ECTL-validointi	CPOC Protocol, kappale I.6.2	TLM-varmenteen päivitys mahdollista myös suojattua verkkoyhteyttä käyttäen. Lisäys: L2: Fyysisesti Italiassa.	Poikkeus sallitaan
4	C-ITS-yksikkö, protokolla	Varmennepolitiikka, ETSI TS 102 941 viite	Poikkeuksia yksikön rekisteröinnissä ja valtuutuksessa voidaan myöntää, mikäli akkreditoitu tarkastaja voi todentaa yksikön turvallisuuden olevan samaa tasoa. Noudatettava ETSI TS 103 097 -standardin sertifikaattiprofiileja.	Poikkeus sallitaan
5	C-ITS-yksikköoperaattori, ISMS	Turvallisuuspolitiikka (1)	Ei ISO 27001 -sertifiointivaatimusta. Käytettävä vertailukelpoista turvallisuuden hallintaprosessia. Lisäys: L2-tasolla ISO 27001 (tai UN R155 tai NIS1 ja NIS2 mukainen) ulkoinen sertifiointi.	Poikkeusta ei sallita

Id	Kohde	Viite	L1-tason lievennys	Siirtymävaiheen jälkeen
6	C-ITS-yksikköoperaattori, yhteentoimivuusauditointi	Turvallisuuspolitiikka (31), (32), (33)	Turvallisuuspolitiikan mukaisen toiminnan auditointi voidaan suorittaa sisäisesti, josta toimitetaan itse toteutettu vaatimustenmukaisuuslausunto PKI-toimijalle. Lisäys: L2: Ulkoinen sertifiointi.	Poikkeusta ei sallita
7	PKI-toimija, yhteentoimivuusauditointi	Varmennepolitiikka, luku 8	Mikäli ISO 27001 -sertifiointia ei ole, niin tulee toimittaa selvitys, joka kuvaa toiminnan tietoturvan olevan standardin vaatimusten tasolla. Lisäys: Käytännössä tietoturvallisuuden hallintajärjestelmän kuvaus ja sisäisen auditoinnin raportti.	Poikkeusta ei sallita
8	PKI-toimija, juurivarmentajan nimeäminen	CPOC-protokolla, luku 1.3.2.2	CPOC-protokollan CertificateID-nimeämiskäytäntö RCA-sertifikaatille ei pakollinen.	Poikkeusta ei sallita.

5 C-ITS-turvatunnusten hallintajärjestelmän käyttöönotto Suomessa

Tässä luvussa käsitellään EU:n keskitetyn C-ITS-turvatunnusten hallintajärjestelmän ja siihen liittyvien C-ITS-turvallisuus- ja varmennepolitiikkavaatimusten aiheuttamia vaatimuksia kansallisen C-ITS-palveluiden arkkitehtuurin toteuttamiselle. Luku sisältää C-ITS-yksiköiden valmistukseen ja hankintaan, juurivarmennepalveluiden perustamiseen, PKI-varmenneratkaisuun liittymiseen sekä C-ITS-yksiköiden operointiin liittyviä vaatimuksia, huomioita ja suosituksia.

Luvussa esitetyt huomiot liittyvät osittain standardeissa ja C-ITS-turvatunnustenhallintajärjestelmän (EU CCMS) määrittelyissä (pääasiassa C-ITS-turvallisuus- ja varmennepolitiikka sekä C-ITS Point of Contact dokumentit) esille tulleisiin vaatimuksiin. Osittain luvussa esitetyt näkökulmat perustuvat selvitystyöryhmän toteuttamiin asiantuntijahaastatteluihin ja kirjallisuuskatsauksen myötä syntyneisiin omiin näkemyksiin.

5.1 C-ITS-yksiköiden hankinta

C-ITS-yksikköoperaattori vastaa operoimiensa yksiköiden käytöstä ja niiden vaatimustenmukaisuudesta. Käytännössä tämä tarkoittaa, että yksikköoperaattorin on syytä varmistaa hankinnan yhteydessä, että hankittavilla yksiköillä on voimassa oleva standardin ISO 15408 mukaisen tietoturvallisuuden tason EAL4 sertifiointi, joka pohjautuu joko komission toteuttamaan tai hyväksymään tietoturvaprofiiliin (Protection Profile). Toimittajalta voi olla myös hyvä pyytää todistus ETSIn järjestämään yhteentoimivuustestiin (ETSI plugtest) osallistumisesta. Huomioitavaa on, että dokumentti ei ole virallinen osoitus C-ITS-yksikön vaatimustenmukaisuudesta, vaan pikemminkin osoitus C-ITS-yksikön valmistajan tekemästä työstä yhteentoimivuuden varmistamiseksi. Mikäli C-ITS-yksikköoperaattori ostaa C-ITS-yksikön, sen on yksinkertaisinta vaatia ja todentaa vaadittujen sertifiointien olemassaolo C-ITS-yksikön hankinnan yhteydessä.

Mikäli C-ITS-yksikköoperaattori päättää kehittää oman C-ITS-yksikön, yksikön kehityksessä on otettava huomioon luvun 4.1 mukaiset vaatimukset.

5.2 C-ITS-keskusyksiköiden hankinta (tai kehitys)

Tämän selvitystyön yhtenä sovittuna painopisteenä oli pitkän kantaman tiedonsiirron käyttö C-ITS-järjestelmän toteuttamisessa. Tämän painopisteen vuoksi tässä luvussa otetaan huomioon erikseen C-ITS-keskusyksiköiden hankintaan tai valmistukseen liittyviä näkökulmia edellisessä luvussa kuvattujen kaikkia C-ITS-yksiköitä koskevien yleisten vaatimusten lisäksi. Osa esille tuoduista näkökulmista perustuu C-Roads-spesifikaatioihin ja osa selvitystyön osana tehtyihin asiantuntijahaastatteluihin.

Euroopan C-ITS-järjestelmän tekninen kehitys, standardointi ja määrittely on hyvin vahvasti perustunut alusta saakka lyhyen kantaman tiedonsiirtoratkaisun hyödyntämiseen, mikä näkyi vahvasti myös vuoden 2019 delegoidussa asetusehdotuksessa (EU C/2019/1789 2019). Hybriditeknologiaan sekä IP-pohjaisen pitkän kantaman tiedonsiirtoon perustuvan C-ITS-järjestelmän määrittelytyötä on tehty C-Roads työryhmän 2 (Technical Aspects) alatyöryhmässä 4 (Hybrid Communication). Tämä työryhmä on määritellyt erillisessä C-Roads-spesifikaatiossa (C-ITS IP

Based Interface Profile 2024) pitkän kantaman tiedonsiirtoratkaisuihin perustuvia arkkitehtuureita ja rajapintoja (viimeisin versio 2.1.0).

Yllä mainittu C-Roads-spesifikaatio sisältää useita tärkeitä pitkän kantaman tiedonsiirron käyttöön liittyviä määrittelyjä, erityisesti C-ITS-keskusyksiköiden ja tiedonvaihtopalvelimien[1] väliseen kommunikaatioon käytettävät protokollat, mahdolliset C-ITS-keskusyksiköiden ja tiedonvaihtopalvelimien väliset verkottumistopologiat sekä C-ITS-luottamusmallin vaikutusalueen rajat IP-verkkoihin pohjautuvassa arkkitehtuurissa. Näitä periaatteita esitetään tarkemmin tämän selvityksen luvuissa 6 ja 7. Tästä C-ITS-keskusyksikköratkaisuja hyödyntävien teknisten arkkitehtuurien määrittelytyöstä huolimatta kyseiseen tekniseen ratkaisuun liittyy vielä niiden kehittämisessä tai hankinnassa huomioitavia näkökulmia.

Valmiina tuotteena hankittavissa olevia täysin C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten mukaisia (etenkään L2-tason vaatimuksiin) C-ITS-keskusyksiköitä ei ole markkinoilla saatavilla. Toki voidaan olettaa, että pitkän kantaman tiedonsiirtoon perustuvien ratkaisujen arkkitehtuurityön edetessä C-Roadsissa (mm. C-ITS-keskusyksikköön liittyvän turvaprofiilin määrittely) ja mahdollisen uuden C-ITS delegoidun asetuksen myötä näitä saadaan suhteellisen pian markkinoille. Taulukossa 5 on esitetty asiantuntijahaastatteluissa esille nousseita näkökulmia markkinoilla tunnistettuihin C-ITS-yksiköihin.

[1] Tiedonvaihtopalvelimet ovat osa EU luottamusmalliin pohjautuvaa C-ITS-toteutusta. Vaikka ne eivät kuulu C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) luottamusalueeseen, ne toimivat kansallisten ja alueellisten C-ITS-palvelutoteutusten välisinä yhdysliikennepisteinä välittäen C-ITS-viestejä niiden välillä. Tiedonvaihtopalvelimien toiminta on määritelty C-Roadsin toimesta (C-ITS IP Based Interface Profile 2024) ja tässä selvitystyössä niitä käsitellään luvussa 7.

Taulukko 5. Asiantuntijahaastatteluihin perustuvia keskusyksiköihin liittyviä huomioita

Selvitystyöryhmän tiedossa oleva tuote, hollantilainen TLEX, tukee osittain C-Roads-vaatimuksia, mutta ei esimerkiksi C-ITS-yksiköiden välisen viestien allekirjoituksen osalta. Toimittaja on kuitenkin jatkossa valmis kehittämään tuotetta Euroopan komission asettamien vaatimusten mukaiseksi. Tuote toimii tällä hetkellä laajimman eurooppalaisen C-ITS-ekosysteemin C-ITS-keskusyksikkönä (Hollannissa käytetään termiä Exchange Node). (Monotch haastattelu 2024)
Tšekkiläisellä yrityksellä, Intens, on C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisella PKI-tuella varustettu C-ITS-keskusyksikkötuote (Intiq), joka sisältää monipuolisesti C-ITS-keskusyksikköominaisuuksia. Intens tunnistaa, että C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) ja C-Roads-määrittelyt ovat vielä vaillinaisia pitkän kantaman tiedonsiirtoon perustuvien järjestelmien C-ITS-keskusyksiköiden osalta. Intens osallistuu C-Roads-yhteistyöhön ja pyrkii itsekin vaikuttamaan sen tulevaan määrittelytyöhön, jotta nämä puutteet korjaantuisivat. (Intens haastattelu 2024)
Norjan tieviranomaisella, Vegvesen, on käynnissä C-ITS-keskusyksikön kehitystyö. C-ITS-keskusyksikön oletetaan olevan ensimmäisessä tuotantokäyttöversiossa vuoden 2025 ensimmäisen puoliskon aikana. Norjalaiset tekevät kehitystyötä etupainotteisesti, vaikka nykyisissä vaatimuksissa ja C-Roads-spesifikaatioissa tunnistetaan puutteita C-ITS-keskusyksikön toteutustapaan liittyen (mm. turvaprofiilin puute, HSM-moduulien käytön vaatimukset). Norjalaisten toteutuksessa ei käytetä konesaliympäristössä HSM-moduuleja, vaan PKI-avainten turvallinen säilö ja viestien allekirjoitus toteutetaan ohjelmallisesti. Tämä toteutus ei ainakaan vielä kehitysvaiheen aikana ole avattu avoimen lähdekoodin alustaksi, kuten norjalaisten toteutus tiedonvaihtopalvelimesta, eikä sen avaamisesta jatkosta ei ole vielä tietoa. (Vegvesen haastattelu 2024)

C-ITS-keskusyksiköiden kehitys

Alla kuvatut näkökulmat on hyvä huomioida, mikäli toimijalla on aikomuksissa lähteä kehittämään omaa C-ITS-keskusyksikköä.

C-ITS-palveluiden teknisen arkkitehtuurin kehitykseen liittyvä vahva lyhyen kantaman tiedonsiirron painote näkyy mm. siinä, että C-ITS-keskusyksikköön liittyvää ISO 15408 Common Criteria turvallisuusprofiilia (PP, Protection Profile) ei ole Euroopan komission puolesta saatavilla. C-ITS-keskusyksikön kehittäjän tulee ainakin vielä selvityksen kirjoittamisen aikaan itse kehittää keskusyksikön tietoturvatason arvioinnin laajuuden määrittelemä turvaprofiili ja hyväksyttää se varmennepolitiikkaviranomaisella ennen varsinaista tuotteen turvallisuustason arviointia.

EU:n C-ITS-palveluiden tekniseen arkkitehtuuriin liittyvät määrittelyt sisältävät C-ITS-yksiköiden teknisen rakenteen osalta vaatimuksen laitepohjaisten turvamoduulien käytöstä (Hardware Security Module, HSM) PKI-avainten säilytyspaikkana sekä allekirjoitusten toteuttajana yksiköiden välisessä viestinnässä. Tienvarsi- ja ajoneuvoyksiköiden osalta tämä tuodaan esille C-ITS-varmennepolitiikassa kyseisten yksiköiden turvaprofiilien määrittelyssä, jotka sisältävät HSM-moduulien tietoturvallisuuden tason arvioinnin. C-ITS-keskusyksiköiden osalta yllä olevan kaltaista määrittelyä ei ole saatavilla liittyen PKI-avainten säilytyksen ratkaisuun.

Asiantuntijahaastatteluiden perusteella osa ajattelee, että HSM-turvamoduulien käyttö on tällä hetkellä vallitseva ajattelu ja tämän vuoksi HSM-moduuleita on

käytettävä myös C-ITS-keskusyksiköissä (Teskalabs haastattelu 2024, Microsec ja Commsignia haastattelu 2024). Osa asiantuntijoista on sitä mieltä, että HSM-moduulit ovat jäänne lyhyen kantaman tiedonsiirtoon perustuvien ratkaisujen määrittelytyöstä, koska HSM-moduulit nimenomaan sisältävät merkittäviä ja kalliita fyysisen tietoturvallisuuden varmentamisen ominaisuuksia (esim. PKI-avainten tuhoaminen, mikäli HSM-moduulia yritetään väkivalloin avata). Saman haastattelun perusteella C-ITS-keskusyksiköiden luonnollinen sijoituspaikka tulisi olla korkean tietoturvatason konesalit, jolloin tämän kaltaiset ominaisuudet ovat joka tapauksessa tarpeettomia (Vegvesen haastattelu 2024). Esille myös tuli, että koska asia on tällä hetkellä epäselvä C-Roads-spesifikaatioiden sekä varmenne- ja turvallisuuspolitiikkojen määrittelyjen osalta, niin tämä asia tullaan nostamaan esille käsiteltäväksi asiaksi C-Roadsin työryhmässä (Almaviva haastattelu 2024).

Yllä esitetyillä PKI-avainten säilytystapaan liittyvillä näkökulmilla on merkittävä vaikutus C-ITS-keskusyksiköiden kehittämiseen, sillä HSM-moduulien käyttö vaikuttaa C-ITS-keskusyksiköiden toteutusarkkitehtuuriin ja voi olla merkittävä kustannuserä keskusyksiköissä, joissa välitetään huomattava määrä viestejä (jopa useampi miljardi päivässä). Tämä saattaa aiheuttaa myös keskusyksikölle skaalautuvuushaasteita. Tämän asian selkeyttäminen vaatii tällä hetkellä lisämäärittelytyötä C-Roadsilta (WG2 Technical Aspects → Security Aspects). Tätä aihetta käsitellään myös tarkemmin tämän selvitystyön seuraavassa luvussa 6.

Selvitystyön työryhmä on tunnistanut myös markkinoilla olevia C-ITS-keskusyksiköiden kehitystyössä hyödynnettäviä avoimia lähdekoodina saatavilla olevia ohjelmistokirjastoja. Yhtenä esimerkkinä saksalainen Vanezza-projekti, jossa on alun perin kehitetty ohjelmistokirjastoja lyhyen kantaman tiedonsiirron ITS-G5-pohjaisiin C-ITS-toteutuksiin. Kehitystyön taustalla on ollut saksalaisessa Ingolstadtin teknisen yliopiston CARISSMA-tutkimuskeskuksessa toteutettava liikenteen turvallisuuden kehittämiseen tähtäävä Car2X-tutkimusohjelma sekä yliopiston tutkija Raphael Riebl. Projektissa kehitettyjä ja avoimesti LGPLv3-lisenssin alaisesti jaettavia (C++) komponentteja voidaan myös hyödyntää pitkän kantaman tiedonsiirron IP-pohjaisissa ratkaisuissa (https://www.vanetza.org/).

Yllä kuvatut seikat eivät varsinaisesti anna C-ITS-keskusyksiköiden toteuttamiseen tai hankintaan selkeitä ohjeita, mutta tuovat esille Euroopassa tehtävää kehitystyötä ja toisaalta tämän hetken C-ITS-määrittelyihin liittyviä epäselvyyksiä ja aukkoja, joita erityisesti C-ITS-keskusyksikön omaan valmistukseen tai C-ITS-keskusyksikön hankintaan tähtäävien organisaatioiden on hyvä ymmärtää.

C-ITS-tiedonvaihtopalvelinta koskeva luku 7 käsittelee tarkemmin oman tiedonvaihtopalvelimen kehittämiseen liittyviä näkökulmia. Luvussa esille tuotavat näkökulmat soveltuvat tiedonvaihtopalvelimen lisäksi myös C-ITS-keskusyksikön kehittämiseen.

5.3 Organisaation tietoturvallisuuden hallintajärjestelmä

Tässä luvussa kerätään yhteen C-ITS-turvallisuuspolitiikan vaatimukset tietoturvallisuuden hallintajärjestelmään ja C-ITS-yksiköiden operointiin liittyen sekä tuodaan esille tähän aiheeseen liittyviä näkökulmia.

C-ITS-yksikköoperaattorin on kehitettävä ja käyttöönotettava standardin ISO 27001 mukainen tietoturvallisuuden hallintajärjestelmä. Hallintajärjestelmä tulee olla ulkoisen auditoinnin avulla sertifioitu. Tietoturvallisuuden

hallintajärjestelmävaatimukset vaihtelevat C-ITS-operaattorin rooliin liittyen (esim. NIS2-alainen toimija tai ajoneuvoteollisuuden edustaja). Nämä vaatimukset on kuvattu tarkemmin tämän selvityksen luvussa 4.2.2.

Tietoturvallisuuden hallintajärjestelmä on yksikköoperaattorina toimivan organisaation sisäinen kehityshanke, jonka avulla kehitetään organisaation tietoturvallisuuden johtamista sekä tietoturvallisuuteen hallintaan liittyviä toiminnallisia prosesseja ja työkaluja. Hallintajärjestelmän tulee ottaa huomioon, ja olla yhdenmukainen, C-ITS-turvallisuuspolitiikan kanssa. Erityisesti tämä koskee C-ITS-turvallisuuspolitiikassa esitettyjä C-ITS-yksiköiden käsittelemän tiedon hallintaan ja luokitteluun sekä riskien hallintaan liittyviä vaatimuksia, jotka on kuvattu tämän selvityksen luvussa 4.2.3.

Hallintajärjestelmän kehittämiseen ja sertifiointiin käytettävä aika vaihtelee hyvin paljon liittyen käytettävissä oleviin resursseihin, johdon sitoutumiseen, hallintajärjestelmän kattavuuteen (koko yrityksen toiminta vai vain osa siitä) sekä tietoturvallisuuden hallinnan lähtötasoon. Keskimääräisesti voidaan sanoa, että tyypillinen sertifiointiin kuluva aika projektin aloittamisesta on noin 1–2 vuotta. Tämä arvio perustuu selvitystyöryhmän käsitykseen asiasta sekä omiin kokemuksiin.

On hyvä huomioida, että tietoturvallisuuden hallintajärjestelmää ei ole C-ITS-turvallisuuspolitiikan mukaisesti välttämätöntä kehittää kattamaan koko organisaation toimintaa. Riittää, että järjestelmän mukainen toiminta koskee nimenomaan C-ITS-yksiköiden operointia. Käytännössä tämä tarkoittaa C-ITS-yksiköiden hallintaa, käyttöönottoa ja ylläpitoa sekä niiden käsittelemän tiedon ja niihin liittyvien järjestelmien riskien hallintaa.

Kansallisen C-ITS-ekosysteemin perustamisessa on myös hyvä huomioida tietoturvallisuuden hallintajärjestelmävaatimusten aiheuttamat välilliset vaikutukset yksityisen sektorin toimijoihin. C-ITS-turvallisuuspolitiikan vaatimukset koskevat lähtökohtaisesti kaikkia C-ITS-yksikköoperaattoreita, jotka tulevat pääasiassa olemaan tienpitäjiä, eli valtioita ja kuntia. Tämä aiheuttaa käytännössä sen, että tilaajille asetetut vaatimukset siirtyvät osaksi valtion ja kuntien C-ITS-järjestelmiä koskevia kilpailutuksia. Näin ne koskevat myös välillisesti yksityisen sektorin toimijoita, jotka tulevaisuudessa toimivat osana C-ITS-yksiköiden kehittämistä, hallintaa, huoltoa ja ylläpitoa. Tilaajille C-ITS-turvallisuuspolitiikan asettamien vaatimusten siirto suoraan toimittajille on käytännössä ainut tapa varmistaa, että C-ITS-ekosysteemin osana toimivat yritykset täyttävät tilaajille asetetut vaatimukset.

Yllä kuvattu alun perin tilaajille asetettujen vaatimusten välillinen siirtyminen toimittajille on näkynyt esimerkiksi NIS2-direktiivin voimaantulon myötä Suomessa. Vuoden 2024 aikana liikennealan kilpailutuksissa on jo selvästi yleistynyt yritysten tietoturvallisuuden hallintaan liittyvät vaatimukset. Vaatimukset ovat linjassa tilaajille asetettuihin NIS2-direktiivin mukaisiin tietoturvallisuuden hallintavaatimuksiin.

Vaatimusten välillinen siirtyminen aiheuttaa yksityiselle sektorille merkittävän määrän tietoturvallisuuden hallinnan kehityspaineita. Tämä saattaa näkyä yritysten ongelmina täyttää vaatimukset ja tämän vuoksi mahdollisuutena vastata toimialan kilpailutuksiin. Vaatimukset vaikuttavat myös toimialalla toimivien yritysten kustannusrakenteeseen tietoturvallisuuden hallintajärjestelmien kehittämisen,

uusien hallinnollisten vaatimusten ja IT-järjestelmien kehittämisen, niiden ylläpidon ja säännöllisesti toteutettavien auditointien kautta.

Tietoturvallisuuden hallintajärjestelmien aiheuttamat kustannukset organisaatoille eivät kuitenkaan rajoitu pelkästään järjestelmän kehitysvaiheeseen ja vuosittaisiin auditointeihin. Tietoturvallisuuden hallintajärjestelmällä on kustannuksia kasvattava vaikutus myös jatkuvassa yrityksen toiminnassa korkeamman tietoturvan hallinnollisen työkuorman (mm. tietoturvan, riskien hallinnan johtamisryhmät, järjestelmän ylläpito ja kehitys), uusien IT-järjestelmien kulujen sekä projekti- ja palvelutoimintaan liittyvien korkeampien tietoturvan hallinnan vaatimusten muodossa. Kaikki nämä yritysten kustannusrakenteen muutokset aiheuttavat luonnollisesti paineita myös laskutushintoihin.

Loppujen lopuksi lisääntyneet tietoturvallisuuden vaatimukset kehittävät toimialan ratkaisujen, tiedon hallinnan ja toiminnan tietoturvallisuuden tasoa, mikä on komission Euroopan laajuinen tavoite. Tietoturva kuitenkin maksaa. Tietoturvallisuuden hallintajärjestelmien aiheuttamia käyttöönoton ja ylläpidon kustannuksia on arvioitu erikseen luvussa 5.7.3.

5.4 PKI-järjestelmän juurivarmennepalvelun vaihtoehdot

C-ITS-yksikköoperaattorin tulee tehdä päätös siitä, minkä C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) varmennepalveluiden toimittajan kanssa C-ITS-yksiköiden rekisteröinti ja varmenteiden hallinta toteutetaan.

Turvatunnusten hallintajärjestelmä mahdollistaa C-ITS-yksiköiden rekisteröinnin minkä tahansa varmennepolitiikkaviranomaisen (CPA) hyväksymän varmennepalveluiden toimittajan järjestelmässä. On mahdollista käyttää maksutonta Euroopan komission ylläpitämää ja Atosin operoimaa EU-juurivarmennepalvelua, saman toimittajan maksullista versiota palvelusta tai sitten muita yksityisten toimijoiden tarjoamia maksullisia juurivarmennepalveluita. Näistä eniten käytetyimpiä ovat tällä hetkellä L0-tason hyväksyttyjen varmenteiden ECTL-listan perusteella unkarilainen Microsec sekä tšekkiläinen Teskalabs. Vuoden 2024 lopussa mahdollistettuja L1-tason varmenteita tarjosi selvitystyön kirjoittamisen hetkellä vasta komission itsensä ylläpitämä juurivarmennepalvelu (EU Root CA) sekä Microsec (CPOC-WEB Logbook: Level 1 Environment). Lopullisen L2-tason mukaisia varmenteita ei ollut vielä rekisteröity käyttöön alkuvuodesta 2025.

Varmennepalvelutoimittajien haastatteluiden perusteella Atosin ylläpitämä ilmainen EU-juurivarmennepalvelu on tarkoitettu pilotointikäyttöön, eikä sitä ole ollut alun perin tarkoitus käyttää laajamittaisissa lopullisissa L2-tason tuotantoympäristöissä (Teskalabs haastattelu 2024, Microsec ja Commsignia haastattelu 2024). EU:n ylläpitämää juurivarmennepalvelua koskeva nykyinen sopimus jatkuu enintään vuoden 2026 loppuun saakka. Palvelun jatkuvuudesta tämän jälkeen ei toistaiseksi ole tietoa. Selvää on kuitenkin, että uuden ITS-direktiivin mukaisissa määrityksissä Euroopan komissiolla ei ole virallista roolia tai vastuuta kyseisen palvelun tuottamisesta. Atos myös kehittää ja tarjoaa PKI-palvelusta maksullista versiota, jossa palvelun teknistä toteutusta ja asiakkaille tarjottavia palveluita kehitetään eteenpäin.

Yksityisten toimijoiden kanssa käytyjen asiantuntijahaastatteluiden mukaan palvelutarjoajien intresseissä on kehittää varmennepalveluita kohti tulevaisuuden laajempia tuotantoympäristöjä ja samalla pyrkiä jatkuvasti kehittämään

varmennepalveluiden hallinnan web-portaaleja sekä muita varmenteiden hallintaan liittyviä ominaisuuksia. Näitä ovat esimerkiksi varmenteiden hallinnan API-palvelut, joiden avulla asiakkaat voivat ohjelmallisesti kehittää ja automatisoida varmenteiden hallintaa. Tämän kehitystoiminnan tavoitteena on kiinteät kumppanuudet asiakkaiden kanssa, mikä sisältää asiakkaiden konsulttina toimimista varmenteiden hallintaan liittyen, parempaa varmenteiden hallinnan räätälöitävyyttä ja web-portaalien avulla saavutettavaa sujuvuutta sekä mahdollisen varmennepalvelutoimintaan liittyvän automatisoinnin, kuten ohjelmallisen API-palveluiden käytön varmenteiden hallintaan. (Teskalabs haastattelu 2024, Microsec ja Commsignia haastattelu 2024)

Haastatteluissa myös todettiin, että oma kansallinen varmennepalvelutoimittaja tarjoaisi C-ITS-yksiköiden laajamittaiseen ja pitkäaikaiseen rekisteröintiin paremman hallinnan, kuin malli, jossa kansalliset C-ITS-operaattorit voivat käyttää täysin vapaasti eurooppalaisia PKI-palveluntarjoajia. Varmennepalvelutoimittaja toimii kansallisten viranomaisten kumppanina ja asiantuntijana C-ITS-yksiköiden rekisteröintitoimintaan liittyen, hallitsee EU turvatunnusten hallintajärjestelmän (EU CCMS) vaatimukset, sertifiointiprosessit ja tarjoaa paremmat mahdollisuudet määritellä kansallisia pelisääntöjä rekisteröintitoimintaan liittyen.

Edellä mainitut hyödyt saavutetaan esimerkiksi tilanteessa, jossa kansallisesti yksi viranomaistaho, kuten toimivaltainen viranomainen koordinoi C-ITS-yksiköille annettavia palvelukohtaisia lupia. Myönnettäessä palvelukohtaisia lupia voidaan varmistaa, että luvan hakijalla on tai se saa käyttäjäoikeudet kansalliseen juurivarmennepalveluun, johon hakija ohjataan toteuttamaan uusien C-ITS-yksiköiden rekisteröinti. Tämä hyöty näkyy erityisesti valtiolliseen käyttöön tarkoitettujen C-ITS-yksiköiden käyttöönotossa, kun toimivaltaiselta viranomaiselta vaadittu yksiköiden käytön valtuutus voidaan yhdistää varmenteiden hakuun kansallisesta keskitetystä palvelusta.

5.5 Kansallinen juurivarmennepalvelu

Tässä luvussa tuodaan esille erilaisia vaihtoehtoja juurivarmennepalvelun toteuttamiseksi. Eri vaihtoehtojen eroja tuodaan esille varmennepalvelutoimittajien kanssa käytyjen haastatteluiden ja markkinoilla olevien ratkaisuvaihtoehtojen pohjalta. (Teskalabs haastattelu 2024, Microsec ja Commsignia haastattelu 2024)

Oman juurivarmennepalvelun hankkiminen liittyy tyypillisesti tilanteisiin, joissa toimija (C-ITS-yksikköoperaattori tai esim. toimivaltainen viranomainen) kokee tarvitsevansa pitkäaikaisempaa C-ITS-yksiköiden rekisteröintiin käytettävää kumppania. Kansallisen juuripalvelun perustaminen olisi tällainen tilanne. Haastatteluiden perusteella tämän kaltaiseen tilanteeseen tunnistetaan seuraavia vaihtoehtoja:

(1) hankkimalla usealle asiakkaalle yhteinen (jaettu) juurivarmennepalvelu SaaS-palveluna (Software as a Service) yksityiseltä palveluntarjoajalta

(2) hankkimalla erillinen vain omaan käyttöön tarkoitettu SaaS-palveluna toteutettu juurivarmennepalveluympäristö yksityiseltä palveluntarjoajalta

(3) toteuttamalla omassa hallussa oleva konesaliratkaisu, johon asennetaan palvelutoimittajan varmenteiden hallintaan tarkoitettu juurivarmennepalveluympäristö (asiakkaan käyttötarkoitukseen varattu paikallinen toteutus)

(4) kehittämällä oma juurivarmennepalveluympäristö (ohjelmistoratkaisu) sekä toteuttamalla se omaan paikalliseen konesaliympäristöön.

Haastateltujen mukaan helpointa ja kustannustehokkainta on ostaa varmennepalvelut vaihtoehdon 1 mukaisesti pilvipohjaisena palveluna (SaaS) jaetusta varmennepalvelutoimittajan ympäristöstä. Tässä tapauksessa juurivarmennepalvelun käyttöönottoon ei tarvita erillisiä varmennepolitiikkaviranomaisen hyväksyttämis- ja auditointitoimia, koska palvelun toimittamiseen käytetty toimintaympäristö on jo läpäissyt nämä vaatimukset. (Teskalabs haastattelu 2024, Microsec ja Commsignia haastattelu 2024)

Toinen tapa on hankkia yksityiseltä palveluntarjoajalta täysin oma, muiden asiakkaiden käyttämästä varmennepalvelutoiminnasta irrallinen, vaihtoehdon 2 mukainen SaaS-varmennepalvelu. Tässä mallissa palvelutoimittaja toteuttaa omaan palvelin- tai pilvipalveluympäristöönsä uuden erillisen SaaS-varmennepalvelun jaetun SaaS-palvelun rinnalle. Toteutus vaatii, että uusi varmennepalvelu rekisteröidään eurooppalaiseen C-ITS-turvatunnusten hallintajärjestelmään (EU CCMS) ja sen tulee käydä läpi kaikki varmennepalvelutoimittajaa koskevat hyväksyttämismenettelyt. Käytännössä palvelutoimittaja hoitaa nämä käyttöönoton yhteydessä tarvittavat ja säännöllisesti toteutettavat hyväksynnät osana oman jaetun SaaS-ympäristön hyväksyntämenettelyjä, mutta tämä lisää silti ympäristöön liittyvää hallinnollista työtä ja kuluja.

Kolmas tapa muistuttaa edellistä ratkaisua siltä osin, että asiakas saa siinäkin käyttöönsä omaan käyttöönsä toteutetun erillisen varmennepalveluympäristön, mutta sillä erolla, että palvelutoimittaja ei toteuta sitä omaan palvelin- tai pilvipalveluympäristöönsä, vaan palvelu toteutetaan asiakkaan osoittamaan paikkaan (asiakkaan oma ja itse hallinnoima konesaliympäristö). Tämä malli on vielä merkittävästi edellistä raskaampi. Varmennepalveluympäristö vaatii tässäkin mallissa kaikki C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaiset hyväksynnät, ja ne kohdistuvat myös palveluympäristön fyysiseen tasoon, jotka auditoidaan osana varmennepalveluympäristön käyttöönottoa (esimerkiksi alivarmentajien fyysinen erottaminen toisistaan). Samalla ympäristön hallinnoinnin vastuu siirtyy enemmän asiakkaalle, joka vastaa ympäristön auditoinneista. Asiakkaalta edellytetään myös standardin ISO 27001 mukaista sertifioitua tietoturvallisuuden hallintajärjestelmää. Toki näihin tehtäviin (pystytys, hallinnointi, auditoinnit) voidaan käyttää kumppania apuna, mutta asiakkaalla on tässä mallissa silti huomattavasti merkittävämpi rooli, kuin edellä kuvatussa vaihtoehdossa 2.

Viimeisessä eli neljännessä mallissa lopputulos on edellisen mallin mukainen, mutta sillä erolla, että oman konesalipalveluympäristön lisäksi myös varmenteiden hallintaan ja jakeluun tarkoitetut ohjelmistoratkaisut toteutetaan itse. Tämä on luonnollisesti pitkä kehitysprosessi ja vaatii toteuttajalta merkittävää erityisosaamista PKI-ympäristöjen toteutuksesta ja hallinnasta nostaen toteutuksen kustannuksia huomattavasti vielä edelliseen malliinkin verrattuna.

Käytännössä juurivarmennepalvelutarjoajien kanssa käytyjen asiantuntijahaastatteluiden pohjalta kansallisissa tai muissa laajoissa C-ITS-toteutuksissa näistä vaihtoehdoista on päädytty joko vaihtoehtoon 1, 2 tai 3. Tarkemmin eri vaihtoehdot käsitellään tämän selvitystyön luvussa 5.7.2, jossa vertaillaan eri palveluita mahdollisten kustannusten ja palveluihin liittyen hyötyjen osalta.

5.6 C-ITS-yksikön rekisteröiminen osaksi C-ITS-turvatunnusten hallintajärjestelmää

Mikäli C-ITS-yksikköä ei ole valmiiksi rekisteröity osaksi C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS) yksikön valmistajan toimesta, niin C-ITS-yksikköoperaattori vastaa tästä toimenpiteestä.

C-ITS-yksikköoperaattori toteuttaa yksiköiden rekisteröimisen jollain edellisessä luvussa mainitulla tavalla: ilmaisen EU-juurivarmennepalvelun, yksityisen varmennepalvelutoimittajan jaetun palvelun tai kansallisesti tai organisaatiokohtaisesti toteutetun erillisen juurivarmennepalvelun avulla.

Yksityiskohtaiset varmenteiden hallintaan liittyvät käytännöt C-ITS-yksiköiden rekisteröinnille vaihtelevat varmennepalvelutoimittajakohtaisesti toteutetun palvelun ominaisuuksien sekä varmennepalvelutoimittajan oman toimintakuvauksen (Certificate Practise Statement, CPS) mukaisesti. Yksiköiden rekisteröimiseen voi liittyä myös paljon kansallisesti sovittuja ja säänneltyjä toimintatapoja. C-Roads on selvityksessään tunnistanut, että käytännöt vaihtelevat paljon eri EU-jäsenmaiden välillä: esimerkiksi palvelukohtaisia lupia on palvelusta ja lainsäädännöstä riippuen saattanut myöntää joko varmennepalvelun tarjoaja, tieoperaattori tai muu viranomainen (Kotilainen et al. 2023).

Varmennepalveluiden toimittajien kanssa käytyjen haastatteluiden perusteella käytännössä varmennepalveluiden toimittajat tällä hetkellä tarjoavat kaikki varmennepalveluiden osuudet (juuri- ja alivarmennepalvelut), joten koko rekisteröintiprosessi voidaan hoitaa valitun yksittäisen juurivarmennepalvelutarjoajan kanssa. (Teskalabs haastattelu 2024, Microsec ja Commsignia haastattelu 2024)

Teknisesti C-ITS-varmennepolitiikan mukaisesti C-ITS-yksikön rekisteröinti toteutetaan alivarmentajien avulla (Enrollment Authority, EA ja Authorization Authority, AA). Rekisteröintipyyntö sisältää C-ITS-yksikköön liittyviä perustietoja (määrä, tarkoitus, aktiivisuusaika) sekä rekisteröivän organisaation perustietoja (yksilöivä tunniste, yhteystiedot, yhteyshenkilöt). Osana rekisteröintiprosessia varmentajalle toimitetaan tiedot ja mahdolliset kansalliset luvat käytettävistä C-ITS-palveluista, joiden perusteella rekisteröijä myöntää C-ITS-yksikölle niin sanotut palvelukohtaiset luvat (Service Specific Permissions, SSP). Samassa yhteydessä luodaan PKI-avainpari, joka tallennetaan palvelukohtaisten lupien lisäksi C-ITS-yksikköön. PKI-avainten avulla yksikkö voi liittyä osaksi EU:n C-ITS-palvelutoteutusten arkkitehtuuria ja toteuttaa palvelukohtaisten lupien mukaisia C-ITS-palveluita. Prosessin toteutustavat vaihtelevat eri juurivarmennepalvelutoimittajien välillä riippuen varmennetoimittajan omasta prosessista ja rekisteröintiin tarjottavan palvelun toteutustavasta.

Aikaisemmin Suomessa toteutetun pilottihankkeen perusteella (Kynsijärvi et al. 2024) Euroopan komission ylläpitämän ilmaisen EU-juurivarmennepalveluiden toimittajan rekisteröintiprosessi perustui hakijan ja palvelutoimittajan väliseen Excel-taulukoiden välittämiseen ja eteni alla kuvatulla tavalla:

(1) C-ITS-yksikön rekisteröintipyynnön lähetys Atos:lle

(2) rekisteröintipyynnön vahvistuksen saaminen ja sopimuspapereiden (EU Root CA & Sub-CA SaaS agreement) vastaanotto varmennepalveluiden toimittajalta

(3) täytetyn ja allekirjoitetun sopimuksen sekä hakijaorganisaation virallisen rekisteröintitodistuksen lähetys varmentajalle

(4) vahvistuksen saaminen varmennepalvelun käytön hyväksynnästä

(5) lopuksi operaattori luo avainparin ja välittää julkisen osan varmennepalvelun toimittajalle, määritellään palvelukohtaiset luvat, yksiköt rekisteröidään PKI-järjestelmään ja C-ITS-yksikköön konfiguroidaan tarvittavat tiedot (avain ja palvelukohtaiset luvat, joiden tulee täsmätä rekisteröitävän yksikön lähettämien C-ITS-viestien kanssa).

Samassa hankkeessa prosessi toteutettiin myös yksityisen juurivarmennepalvelutarjoajan avulla. Hankkeen loppuraportti toi esille, että C-ITS-yksiköiden rekisteröintiin ja varmenteiden hallintaan tarkoitettu yksityisen palvelutarjoajan tarjoama web-pohjainen portaali helpotti ja nopeutti C-ITS-yksiköiden rekisteröintiprosessia. Rekisteröintiä nopeutti myös C-ITS-yksiköiden valmistajan toteuttamat rekisteröinnin automatisoidut osuudet (yksikköön toteutetut ”skriptit”), joiden avulla C-ITS-yksikkö vaihtoi tietoja automaattisesti varmennepalvelutarjoajan (Microsec) API-rajapinnan kanssa.

Kummassakin tapauksessa, EU-juurivarmennepalvelu ja yksityisen palvelu, rekisteröijälle jäi myös manuaalisia C-ITS-yksikön konfigurointiin liittyviä työvaiheita.

Juurivarmennepalvelun valinnassa on hyvä huomioida seuraavia seikkoja.

- EU-juurivarmennepalvelun jatkosta ei ole täyttä varmuutta. Sitä ei kuitenkaan ole lähtökohtaisesti tarkoitettu laajoihin tuotantoympäristöihin, ja Excel-tiedostojen välittämiseen perustuva palvelun käyttö on tällä hetkellä hieman hidasta ja kömpelöä verrattuna kaupallisten toimijoiden palveluihin. Palvelu on ilmaista.
- Yksityiset toimijat tarjoavat C-ITS-yksiköiden rekisteröimiseen ja varmennepalveluiden hallintaan yksinkertaisempia web-pohjaisia palveluportaaleja (myös ilmaisen EU-juurivarmennepalvelun toimittaja Atos). Yksityisten toimijoiden varmennepalvelut ovat maksullisia, mutta toimijat saattavat tarjota myös pienimuotoisiin ja yksittäisiin L0-tason pilotteihin joko ilmaisia tai erittäin kohtuuhintaisia palveluita.
- Jos kyseessä on pienimuotoinen tai kertaluontoinen ympäristö, on helpointa käyttää juurivarmennepalvelutarjoajien tarjoamaa jaettua palveluympäristöä. Palveluntarjoajien kanssa käytyjen keskusteluiden perusteella tämä malli on varsin toimiva isommissakin ympäristöissä.
- Mikäli varmennepalvelu halutaan vain omaan käyttöön toteutetun palveluympäristön avulla, voidaan käyttää edelleen SaaS-pohjaista palvelumallia, jossa palvelutoimittaja perustaa asiakkaalle oman erillisen palveluympäristön. Tällä mallilla on toteutettu esimerkiksi kansallisia (mm. Tšekki), kaupunkikohtaisia (Hampuri) tai organisaatiokohtaisia (mm. Autobahn tai ASFINAG) varmennepalveluita.
- Jos varmennepalvelun toteuttamisessa SaaS-mallilla nähdään kansalliseen tai organisaation turvallisuuteen liittyviä riskejä, voidaan harkita oman maan tai organisaation sisäiseen konesaliympäristöön perustettavaa juurivarmennepalvelua (paikallisen toteutuksen malli). Tämän perustamista varten on kuitenkin varauduttava korkeampiin kuluihin, korkean tietoturvallisuustason konesaliympäristön perustamiseen (tai hankintaan), isompaan omaan rooliin liittyen

ympäristön hallinnointiin ja C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisiin jatkuviin hyväksyttämismenettelyihin.

5.7 Kustannusanalyysi

Tässä luvussa käsitellään C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) käyttöönoton aiheuttamia kustannuksia kansallisella tasolla. Turvatunnusten hallintajärjestelmän käyttöönoton aiheuttamat kustannukset voidaan jakaa käytännössä seuraaviin osa-alueisiin.

(1) Kansallisen C-ITS-keskusyksikön ja tiedonvaihtopalvelimen käyttöönotto ja operointi.

(2) Juurivarmennepalvelut, mahdollisen keskitetyn kansallisen juurivarmennepalvelun perustaminen ja varmennepalveluiden käyttö.

(3) C-ITS-yksikköoperaattoreille syntyvät kustannukset turvallisuus- ja varmennepolitiikan vaatimuksiin liittyen.

Kohdan 1 mukainen kustannuselementti perustuu tätä selvitystyötä vahvasti ohjaavaan pitkän kantaman tiedonsiirtoratkaisuun liittyvään tutkimuslinjaan. Kohtien 2 ja 3 mukaiset kustannuselementit eivät ole riippuvaisia C-ITS-palveluiden arkkitehtuurin teknisestä toteutustavasta (pitkän tai lyhyen kantaman tiedonsiirtovaihtoehto).

Kustannusten syntymiseen ja kohdentumiseen liittyy myös merkittävä määrä kansallisia valintoja, jotka vaikuttavat kustannusten syntyyn ja jakautumiseen eri C-ITS-ekosysteemin jäsenten välillä. Näitä valintoja tuodaan esille osittain tässä kustannusanalyysissä, mutta niitä on tuotu osittain esille myös jo aiemmissa tämän selvityksen luvuissa.

On myös hyvä huomioida, että nämä kustannuskomponentit eivät vielä tarkoita, että yksikään C-ITS-palvelu olisi saatu käyttöön ja tuotantoon. Nämä kustannukset ovat C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) sekä turvallisuus- ja varmennepolitiikoiden mukaisen C-ITS-järjestelmän käyttöönottamiseksi tarvittavia perusinfrastruktuuripalveluita sekä toimijoille asetettuja vaatimuksia varsinaisten C-ITS-palveluiden kehittämiselle.

5.7.1 C-ITS-keskusyksikkö ja tiedonvaihtopalvelin

C-ITS-keskusyksikön ja tiedonvaihtopalvelimen toteutukseen voidaan tunnistaa karkeasti kolme erilaista toteutustapaa: (1) oma kehitystyö, (2) markkinoilta ostettu tuote tai palvelu, (3) avoimen lähdekoodin yhteisöllinen kehittäminen.

Kansallisen C-ITS-keskusyksikön toteutukseen mahdollisesti liittyy kiinteästi myös kansallisen tiedonvaihtopalvelimen toteutus. Tiedonvaihtopalvelimen tarkempia vaatimuksia käsitellään tämän selvityksen luvussa 7.

Taulukko 6. Fintraffic Tie Oy:n kanssa käydyn asiantuntijahaastattelun perusteella arvioidut kustannukset C-ITS-keskusyksikön ja tiedonvaihtopalvelimen omaan kehitystyöhön perustuvasta kehityksestä ja käyttöönotosta (Fintraffic haastattelu 2024)

Kustannuslaji	Selitys	Kustannusarvio
C-ITS-keskusyksikön ja tiedonvaihtopalvelimen kehitystyö	Keskusyksikön kehitystyön taustalla arvio n. 2 vuotta kestävästä kehitystyöhankkeesta, jonka minimiresursointi 7 täyttä henkilötyöpanosta (full-time equivalent, FTE). Tiimi: 1 kpl tekninen pääarkkitehti, 2 kpl back-end kehittäjiä, 1 kpl tietovarastoasiantuntija, 1 kpl UI-kehittäjä ja kahden täyden henkilötyöpanoksen verran muita tehtäviä ja rooleja (projektinhallinta, laatu, UX-suunnittelu, pilvi- tai palvelinarkkitehtuuri, rajapintakehitys). Työhön sisältyy myös ISO 15408 (Common Criteria) mukainen tietoturvaprofiilin määrittely ja hyväksyntä, tietoturvatason arviointi sekä ETSI:n mahdollistama yhteentoimivuuden testaus (ETSI Plugtest -tapahtumaan osallistuminen).	n. 2 000 000–2 500 000 euroa
Jatkuvat kustannukset	ICT-infrastruktuurin 24/7-operointi, ITIL-mukaiset (IT Infrastructure Library) hallintapalvelut (häiriönhallinta, ongelmanhallinta jne.), 15 min reagointiaika (NIS2 kriittinen järjestelmä). Arvio 300 000 euroa/vuosi. Alustojen tietoturvan hallintapalvelu, versionhallinta, uusien tietoturvapäivitysten suunnittelu, testaus ja käyttöönotto kuukausittain. Arvio noin 200 000 euroa/vuosi. Kapasiteettipalvelut (pilvipalvelu- tai palvelinalustat, fyysinen kahdennus, kuormantasaus, tietokantakapasiteetti, tietoturvamoduulit, tietoliikenne). Arvio 150 000 euroa/vuosi. Jatkuva ohjelmiston elinkaarenhallinta (ohjelmistovirheiden korjaukset ja ohjelmistojen tietoturvapäivitykset), uudet ominaisuudet ja välttämättömät kehitystarpeet (mm. EU- ja kansalliset integraatiot), jatkuva noin kahden henkilön jatkuva kehityspanos. Arvio 250 000 euroa/vuosi	n. 900 000 euroa/vuosi
Huomioita: C-ITS-keskusyksikön ja tiedonvaihtopalvelimen kehitystyöhön esitetty kahden vuoden aika on aktiivinen ja tehokas määrittely- ja kehitysaika. Projektiin liittyy hyvin todennäköisesti useita viiveitä, esimerkiksi päätöksentekoon liittyviä sekä Common Criteria		

arvioinnit sekä ETSI-yhteentoimivuustestaukset, jotka pidentävät projektin todellista toteutusaikaa.

Omaa kehitystyötä on mahdollista nopeuttaa hyödyntämällä mahdollisia avoimen lähdekoodin alustoja, joita voi ottaa oman kehitystyön pohjaksi ja joiden pohjalta voi lähteä kehittämään omaa kooditoteutusta. Kehitystyön nopeutumisen vastapainona on ottaa omalle vastuulle kehitystyön pohjaksi usein hyvinkin laaja ohjelmistototeutus mahdollisine ohjelmistovirheineen ja tietoturvaongelmineen. Alkuperäisen koodin kehittämä avoimen lähdekoodin yhteisö (tai muu toimija) ei usein tarjoa alkuperäisen kooditoteutuksen osalta tukea kehittäjälle, joka aloittaa oman toteutuksen kehittämisen avoimen koodin pohjalle (joskaan tähän tekoon ei välttämättä liity myöskään mitään negatiivista, vaan on hyvin yleinen toimenpide avoimen lähdekoodin maailmassa).

Toinen avoimen lähdekoodin vaihtoehto on perustaa tai liittyä yhteisön tekemiseen, jota on kuvattu alla omana vaihtoehtona hieman enemmän sekä erityisesti tämän selvityksen luvussa 7.

Taulukko 7. Alla on arvioitu C-ITS-keskusyksikön ja tiedonvaihtopalvelimen valmiin tuotteen hankinnan kustannusten rakennetta. Nämä arviot perustuvat selvitystyöryhmän omaan arvioon.

Kustannuslaji	Selitys	Kustannusarvio
C-ITS-keskusyksikön ja tiedonvaihtopalvelimen käyttöönotto	Palvelutoimittaja perustaa omaan palveluympäristöönsä asiakaskohtaisen toimialueen (jaettu palvelu, jossa asiakkaat eritelty käyttöoikeushallinon keinoin) tai asiakaskohtaisen erillisen paikallisen toimintaympäristön (myös laitealustan puolesta).	n. 500 000–1 000 000 euroa
Jatkuvat kustannukset	Palveluna toimitetun ympäristön käyttöoikeuslisenssi.	n. 250 000–500 000 euroa/vuosi

Huomioita:

Palveluna toimitetun ympäristön hinnoitteluperiaatteet voivat vaihdella merkittävästi palvelutoimittajakohtaisesti. Kustannuksia saatetaan sitoa järjestelmään liitettyjen C-ITS-yksiköiden määrän perusteella tai käytettävän kapasiteetin perusteella. Kustannusmalleihin voi myös merkittävästi vaikuttaa tilaajan tekemillä kilpailutukseen liitettävillä määrittelyillä. Hinnoittelu voidaan pyytää ilmoittamaan esimerkiksi jollakin tietyllä rakenteella, kuten kiinteä vuosikustannus vuosikohtaisella korotusvaralla tai hinnan muodostuminen siihen liitettyjen laitemäärien mukaisesti.

Yksityisen sektorin hinnoitteluun ja hintakehitykseen vaikuttaa myös alalle syntyvien tuotteiden määrä (kilpailu).

Tuotehankintaan liittyviä etuja on selkeästi kevyempi palvelun käynnistäminen sekä tuotteen automaattinen kehittyminen ja uusien vaatimusten sekä standardien mukaisuus ilman erillisiä kustannuksia. Näiden etujen vastapainona on tuotteen kehitykseen ja sen priorisointiin liittyvä heikompi hallinta.

Taulukko 8. Alla on arvioitu C-ITS-keskusyksikön ja tiedonvaihtopalvelimen toteuttamista osana avoimen lähdekoodin yhteisöä.

Kustannuslaji	Selitys	Kustannusarvio
C-ITS-keskusyksikön/tiedonvaihtopalvelimen kehitystyö	Käytännössä varsinaisen tuotteen tai ratkaisun kehitystyön vaatimukset ovat vähintään samat kuin omaan kehitystyöhön perustuvassa, jotka esiteltiin taulukossa 6. Tekemisen malli on erilainen, mikä aiheuttaa kustannusten arviointiin paljon vaikeuksia. Käytännössä työtä tehdään yhteisön osana, jolloin kaikki jäsenet antavat oman panoksensa kehitystyöhön. Lähtökohtaisesti voidaan siis ajatella, että oman osuuden kustannus pienenee yksin tekemiseen verrattuna. Toisaalta todellinen kustannus riippuu esimerkiksi yhteisön koosta, tavoitteista, yhteneväisestä visiosta tuotteen suhteen, halusta panostaa yhteiskehittämiseen, yhteiskehityksen hallinnon onnistumisesta jne.	-
Jatkuvat kustannukset	Jatkokehittämisvaiheen ja ylläpidon kustannusten arviointiin liittyy paljon samanlaisia vaikeuksia kuin edelliseen kehitysvaiheeseen.	-

Huomioita:

Yhteisömäisen tekemisen periaatteen taustalla voisi olla, että useampi maa (esim. Pohjoismaat) haluaisi kehittää C-ITS-keskusyksikköä ja tiedonvaihtopalvelinta yhteistyössä. Tämä tarkoittaisi yhteisen avoimen lähdekoodin yhteisön perustamista, johon liittyisi myös yhteisesti sovittava hallinnollinen malli.

Tämän kaltaisten avoimen yhteisön hallinnon hoitamiseen yleensä ostetaan joku palvelutoimija, joiden erityisosaamista on tuottaa avoimen lähdekoodin yhteisön toimintaan liittyviä hallinnointipalveluita (ohjelmiston säilytys- ja versionhallinta-alustat, kollaboraatio, kehitystyön keskitetty ohjaus).

Yhteisömäisessä tekemisessä on merkittävä määrä hyötyjä verrattuna pelkkään avoimen lähdekoodin alustan koodien hyödyntämiseen osana omaa kehitystä. Yhteisön sisällä kukin vastaa omasta osuudestaan ja tarjoaa tukea muille yhteisön jäsenille mahdollisissa omaan osuuteen liittyvissä ongelmatilanteissa. Yhteisö itse sisäisesti huolehtii kaikkien tekemien osuuksien yhteentoimivuuden varmistamisesta ja testaa yhdessä rakentuvaa kokonaisuutta. Yhteisön sisällä toimiminen tuottaa siis paremman tuen lopullisen ratkaisun lähdekoodiin ja mikäli yhteisön jäsenillä on selkeä sekä yhteneväinen näkemys kehitettävän ratkaisun suunnasta, niin kaikki hyötyvät täysimääräisesti toistensa tekemästä työstä.

Yhtenä yhteisötekemisen haittana tunnistetaan kehitystyön aloittamisen hitaus. Yhteisön perustaminen ja yhteisestä hallinnosta sekä kehitystyön periaatteiden sopiminen voi olla aikaa vievää.

Näitä avoimen lähdekoodin yhteisökehittämisen piirteitä käydään vielä tarkemmin läpi tämän selvityksen luvussa 7.

5.7.2 Juurivarmennepalvelut

Juurivarmennepalveluiden tuottamat kustannukset vaihtelevat hyvin paljon sen suhteen, minkälainen toteutusmalli kansallisesti valitaan. Erityisesti tämä vaikuttaa kustannusten jakautumiseen eri toimijoiden välillä ja toisaalta mahdollisuuksiin hallita C-ITS-yksiköiden käyttöä, rekisteröintiä ja palvelukohtaisten lupien hallintaa.

On mahdollista valita malli, jossa ei perusteta kansallista juurivarmennepalvelua, vaan annetaan kunkin tahon hoitaa varmennetoiminta oman haluamansa juurivarmentajan kanssa. C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) toimintaperiaate mahdollistaa tämän, ja palvelukohtaisten lupienkin hallinnan osalta tämä malli on mahdollinen. Luvat tulee hakea yhdeltä (sovitulta) valtionhallinnon taholta ja lupien saamisesta tulee luovuttaa todiste luvan hakijalle, jotta valittu juurivarmennepalvelun tuottaja voi rekisteröinnin yhteydessä antaa hyväksyttyjen C-ITS-palveluiden luvat rekisteröitäville C-ITS-yksiköille.

Toisena vaihtoehtona on perustaa valtionhallinnon toimesta Suomeen oma kansallinen juurivarmennepalvelu, jota kaikki suomalaiset tienpitäjät käyttävät. Tätä voidaan myös päättää tarjota muillekin C-ITS-ekosysteemin jäsenille. Keskitetty malli parantaa palvelukohtaisten lupien ja juurivarmenteiden jakamisen hallintaa, kun hallintaprosessi voidaan kansallisesti suunnitella sujuvaksi ja toisaalta jokaisen C-ITS-yksiköitä rekisteröivän suomalaisen toimijan (C-ITS-yksikköoperaattorin) ei tarvitse aloittaa omaa toimintaansa juurivarmennepalvelun etsimisellä, kilpailuttamisella ja sopimuksen solmimisella. Tässäkin mallissa kansallisen juurivarmennepalvelun käytön maksullisuudesta voidaan tehdä omia päätöksiä.

Ilmaista EU:n juurivarmennepalvelua ei oteta tässä arvioinnissa huomioon, sillä selvitystyöryhmän sekä asiantuntijahaastatteluiden pohjalta saatu käsitys on, että tätä palvelua ei ole tarkoitettu laajamittaisten ja pitkäaikaisten C-ITS-järjestelmien varmennepalveluihin.

Taulukko 9. Erilaisia kansallisen juurivarmennepalvelun toteuttamisen kustannusarvioita. Arviot perustuvat osittain juurivarmennepalvelutoimittajien kanssa käytyihin asiantuntijahaastatteluihin (Teskalabs haastattelu 2024, Microsec ja Commsignia haastattelu 2024.

Kustannuslaji	Selitys	Kustannusarvio
Jaettu SaaS PKI juurivarmennepalvelun perustaminen	Juurivarmennepalvelu ostetaan pilvipalvelupohjaisena palveluna palvelutoimittajalta, joka perustaa uuden asiakkuuden varmennepalveluun, perustaa pääkäyttäjät ja käyttäjät asiakkaan tarpeen mukaisesti. Toimintaympäristö on jaettu muiden kyseisen palveluntarjoajan asiakkaiden kanssa.	n. 10 000 euroa
Jaettu SaaS PKI juurivarmennepalvelun käyttökustannukset	SaaS-palvelu tarjotaan täysin palveluna, eikä asiakkaan tarvitse huolehtia sen infrastruktuuriin liittyvistä kuluista, järjestelmän kehityksestä, C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten muuttumisesta tai vuosittaisista auditoinneista. Tilaajalla on mahdollisuus myös vaikuttaa näihin kuluihin kilpailutuksen vaatimusten avulla (esim. vaatimuksena kiinteä kuukausihinta koko sopimuskauden ajan tai hinnan perusteena rekisteröityjen C-ITS-yksiköiden määrä jne.). Asiantuntijahaastatteluiden mukaan yleinen hinnoitteluperuste on rekisteröityjen C-ITS-yksiköiden määrä. Toisaalta toisenlaisiakin malleja on palvelutoimittajille tullut vastaan, esim. vuosittaiset kiinteät kustannukset ennalta arvioitujen laitemäärien mukaisesti. Käyttökustannusten arvioinnin perustana on ollut oletus, että kansallinen C-ITS-ekosysteemi on aloittanut toimintansa ja ohittanut kehityksensä alkuvaiheen, jossa rekisteröityjen laitteiden määrä voi olla hyvin pieni.	n. 25 000–100 000 euroa
Asiakaskohtainen SaaS PKI juurivarmennepalvelun perustaminen	Juurivarmennepalvelu ostetaan pilvipalvelupohjaisena palveluna palvelutoimittajalta, joka perustaa uuden asiakaskohtaisen varmennepalveluympäristön. Palveluntarjoaja hyväksyttää uuden perustetun juurivarmennepalvelun osaksi C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS) ja perustaa ohjelmistot ja asiakkuutta varten tarvittavat käyttäjätunnukset ja rakenteet. Malli antaa paremmat mahdollisuudet mm. käyttäjäryhmien hallinnan monipuolisuuden osalta. Hallintaympäristöön voidaan perustaa myös useita pääkäyttäjiä, joilla on oikeus vain oman ryhmänsä laitenäkymään (esim. kaupunki).	n. 25 000–100 000 euroa

Kustannuslaji	Selitys	Kustannusarvio
Asiakaskohtainen SaaS PKI juurivarmennepalvelun käyttökustannukset	Palvelutoimittaja operoi ja tarjoaa varmennepalvelua omalta palvelin- tai pilvipalvelualustaltaan, tarjoaa asiakkaalle varmenteiden ja käyttäjien hallintaan työkalut sekä tukipalvelut järjestelmän käyttöön. Palvelutoimittaja myös vastaa palveluna C-ITS-turvatunnusten hallintajärjestelmään (EU CCMS) liittyvistä vuosittaisista auditointivaatimuksista sekä mahdollisista uusiin vaatimuksiin liittyvistä muutostarpeista.	n. 50 000–200 000 euroa
Paikallinen PKI juurivarmennepalvelun perustaminen	Juurivarmennepalveluiden paikallinen toteutusvaihtoehto perustuu asiakkaan valitsemaan sijaintiin perustettavaan täydellisen juuripalveluinfrastruktuurin perustamiseen sisältäen sekä palvelininfrastruktuurin sekä ohjelmistojen asennuksen. Tällä mallilla saa täydellisen hallinnan juurivarmennepalveluun, mutta se vaatii merkittävän määrän erikoisosaamista, vaatii huomattavia investointeja laitteistoon, kuten HSM-moduuleihin, joihin avaimet tallennetaan, sekä redundanttiseen ja maantieteellisesti hajautettuun arkkitehtuuriin. Alivarmennuspalvelut tulee pitää myös fyysisesti toisistaan erillään. Juurivarmennepalveluympäristö tulee hyväksyttää C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten mukaisesti kaikkien tasojen osalta (konesali-, palvelin- ja ohjelmistoinfrastruktuuri).	n. 500 000–1 000 000 euroa
Paikallinen PKI juurivarmennepalvelun käyttökustannukset	Oman paikallisesti toteutetun juurivarmennepalvelun käyttökustannukset määräytyvät hyvin eri tavalla kuin SaaS-palveluna hankittavan. Tässä mallissa jatkuvat kustannukset muodostuvat kapasiteettipalveluiden käyttökuluista (palvelimet, tietokannat, palomuurit, tietoliikenne sekä järjestelmän jatkuvat 24/7 valvonta- ja hallintapalvelut, kriittisen reagointiajan reagointipalvelut, ITIL-prosessien mukainen hallintapalvelu) sekä ympäristön jatkuvista auditointivaatimuksista ja kaikkien näiden toimintojen hoitamiseen vaadittavasta asiantuntijatyöstä. Merkittävä osa kaikista operointiin liittyvistä vastuista siirtyy siis asiakkaan harteille, vaikka sekä operointiin, C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten täyttymiseen ja vuosittaisiin auditointeihin on mahdollista saada ulkoiselta kumppanilta tukipalveluita. Kustannusarvio perustuu C-ITS-keskusyksikön ja tiedonvaihtopalvelimen jatkuvien palveluiden hinnoitteluarvioon sekä arvioon vuosittaisten auditointien ja muiden C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten vaikutuksista.	n. 250 000–500 000 euroa

5.7.3 C-ITS-yksiköiden operointi

C-ITS-yksiköiden operaattorien kustannukset koostuvat pääosin varsinaisten C-ITS-yksiköiden hankinta- tai kehityskuluista, C-ITS-palveluiden kehitys- ja käyttöönottokuluista sekä C-ITS-yksiköiden operointiin liittyvistä kuluista.

Tässä luvussa ei oteta kantaa C-ITS-palveluiden käyttöönottokustannuksiin (yksiköiden hankinta ja käyttöönotto), vaan ainoastaan C-ITS-turvallisuuspolitiikan asettamien vaatimusten aiheuttamiin kustannuksiin C-ITS-yksikköoperaattorille. Käytännössä tämä tarkoittaa tietoturvallisuuden hallintajärjestelmien sertifiointivaatimusta, jotka on kuvattu tämän selvityksen luvussa 4.2.2.

Alla on kuvattu lyhyesti kertauksena C-ITS-turvallisuuspolitiikan asettamat tietoturvallisuuden hallintajärjestelmiin liittyvät vaatimukset C-ITS-yksikköoperaattoreille:

- Yleinen vaatimus on standardin ISO 27001 mukainen ja sertifioitu tietoturvallisuuden hallintajärjestelmä.
- Ajoneuvoyksiköitä operoivat tahot voivat korvata tämän vaatimuksen E-säännön UN R155 mukaisesti sertifioidulla kyberturvallisuuden hallintajärjestelmällä (UN Regulation No. 155 2021).
- Olennaista liikennepalvelua operoivat tahot voivat soveltaa tietoturvallisuuden hallintaan NIS1- ja NIS2-kyberturvallisuusdirektiivien mukaisia vaatimuksia.

Tässä kustannusarviossa ei ole tehty eroa näiden eri järjestelmien sertifioinnin ja sertifikaatin ylläpitämisen kustannusten osalta. Kustannusarviot perustuvat alalla yleisesti olevaan tietoon ja käytettyihin kustannusarvioihin sekä selvitystyöryhmän oman asiantuntemukseen.

Taulukko 10. C-ITS-yksikköoperaattoreille aiheutuvia kustannuksia tietoturvallisuuden hallintajärjestelmien kehittämisestä, sertifioinnista sekä hallintajärjestelmän ja sertifiointien ylläpitämisestä.

Kustannuslaji	Selitys	Kustannusarvio
Tietoturvallisuuden hallintajärjestelmän kehitys ja sertifiointi	Tietoturvallisuuden hallintajärjestelmän kehittäminen sisältäen organisaation tietoturvallisuuden hallinta- ja johtamismallien kehitys, toimintatapojen kehittäminen, uudet mahdolliset IT-laite- ja järjestelmäinvestoinnit, mahdollisesti tarvittavat konsulttipalvelut sekä organisaation projektiin käyttämä aika. Projektin kestoksi yleisesti arvioidaan n. 1–2 vuotta riippuen organisaation koosta ja tietoturvallisuuden hallinnan lähtötasosta.	n. 50 000–100 000 euroa
Tietoturvallisuuden hallintajärjestelmän ylläpitokustannukset	Tämä kohta sisältää lähinnä tietoturvallisuuden hallinta järjestelmän vuosittaisiin auditointeihin kuluvan työajan sekä auditointimaksut.	n. 10 000–30 000 Eur

Huomioita:

Yllä oleva ylläpitokustannusten osuus ei ota kantaa yritysten jatkuvan operatiivisen toiminnan kustannusrakenteeseen, johon tietoturvallisuuden hallintajärjestelmillä on tyypillisesti yrityksen toiminnan sisäisiä kustannuksia nostava vaikutus (riippuen yrityksen tietoturvallisuuden hallinnan lähtötasosta ennen sertifiointia). Näitä vaikutuksia ovat mm. yrityksen toiminnassa näkyvä korkeampi tietoturvan hallinnollinen työkuorma (mm. tietoturvan, riskien hallinnan johtamisryhmät, suunnittelutyössä näkyvät uudet tietoturvan hallintaan liittyvät käytännöt sekä henkilöstön koulutus ja ohjeistus tietoturvallisuuden hallintaan liittyen), uusien IT-järjestelmien käyttökustannukset sekä hallintajärjestelmän asettamat projekti- ja palvelutoimintaan liittyvät korkeammat tietoturvan hallinnan vaatimukset. Tietoturvallisuuden hallintaan liittyvien uusien tehtävien aiheuttamat kustannukset ovat vahvasti sidoksissa organisaation kokoon. Nämä uudet tehtävät, toimintaryhmät ja työssä huomioitavat uudet käytännöt aiheuttavat tyypillisesti moninkertaisesti enemmän kustannuksia kuin yllä taulukossa esitetty järjestelmän auditoinnin ja järjestelmän ylläpidon kustannukset. Esimerkiksi, jos 50 hengen organisaatiossa uudet käytännöt vievät jokaiselta työntekijältä 4 tunnin verran enemmän aikaa kuukausittain, niin tämä tarkoittaisi lähes 150 000 euron lisäkustannuksia vuosittain tietoturvan hallintaan liittyen (4 x 50 x 12 x 60 euroa/tunti).

Luvussa 5.3 kuvattiin sertifiointivaatimusten välillisiä vaikutuksia koko älykkään liikenteen toimialaan. Nämä vaatimukset koskevat myös C-ITS-palveluiden parissa toimivia yrityksiä, kun C-ITS-yksikköoperaattoreita koskevat sertifiointivaatimukset hyvin todennäköisesti siirtyvät koskemaan myös yksityisen sektorin toimijoita, jotka toimittavat ratkaisuja tai palveluita C-ITS-yksikköoperaattoreille liittyen C-ITS-järjestelmien kehittämiseen, operointiin, huoltoon ja ylläpitoon.

Tässä kohdassa kuvattuja C-ITS-yksikköoperaattoreille koituvia kustannuksia voidaan pyrkiä minimoimaan teknisen arkkitehtuurin suunnittelulla. Pitkän kantaman tiedonsiirtoon perustuvassa vaihtoehdossa voidaan kehittää ratkaisuja niin, että keskitetään C-ITS-yksiköiden operointivastuuta pelkästään C-ITS-keskusyksikön operoinnista vastaavalle taholle. Tällä tarkoitetaan, että vasta C-ITS-keskusyksikkö muodostaa C-ITS-viestit, jolloin lähtötiedot viestien muodostamiselle toimitetaan muilla tavoilla. Tästä esimerkkeinä voivat olla vaikka ajantasaista liikennetietoa ja liikenneturvallisuuteen liittyviä vähimmäistietoja jakavan kansallisen yhteyspisteen (National Access Point, NAP) hyödyntäminen ja liikennevalotietojen lähetys kansalliselle C-ITS-keskusyksikölle kansallisesti määritellyn tietoturvallisen tiedonsiirtotavan avulla (ei C-ITS-tienvarsilaitteen avulla).

Kansallisen yhteyspisteen hyödyntämiseen liittyvänä esimerkkinä toimii ITS-direktiivin vaatimus SRTI- ja RTTI-tietojen välittämisestä yhteyspisteelle. Tietyömaiden C-ITS-varoitusviestipalvelut (Roadworks Warning, RWW) voidaan toteuttaa niin, että tieurakointiyhtiöiltä vaaditaan osana kilpailutuksia (vain) SRTI-tietojen välittäminen kansalliseen yhteyspisteeseen. Kansallisen yhteyspisteen kautta tiedot voidaan siirtää kansalliseen C-ITS-keskusyksikköön sekä muihin yksityisten toimijoiden ylläpitämiin C-ITS-palveluntarjoajarajapintoihin, jotka muodostavat tietojen avulla tietyömaiden C-ITS-varoitusviestit ja jakelevat niitä matkaviestinverkkojen välityksellä tietyömaita lähestyville ajoneuvoille. Näin huoltourakoitsijalle ei koidu C-ITS-yksikköoperointiin liittyviä vaatimuksia eikä kustannuksia (esim. C-ITS-tienvarsiyksiköiden hankinta ja niiden operointiin liittyvät vaatimukset). Tätä aihetta käsitellään tarkemmin selvitystyön luvussa 11.

6 C-ITS-keskusyksiköt ja viestien allekirjoittaminen

6.1 Johdanto

C-ITS-keskusyksikkö on yksi neljästä standardin ETSI EN 302 665 viitearkkitehtuurin C-ITS-yksikkötyypistä. C-ITS-keskusyksiköt ovat pilvipalveluissa tai konesaleissa toimivia ohjelmistoratkaisuja ja toimivat tärkeinä C-ITS-palvelutoteutusten arkkitehtuureiden taustajärjestelminä. Keskusyksiköillä on keskeinen rooli C-ITS-palveluiden toiminnassa. Ne keräävät tietoa liikenneverkon ja ajoneuvojen tilasta, muodostavat C-ITS-viestejä monipuolisesti erilaisten lähtötietojen perusteella, välittävät viestejä alueellisten C-ITS-järjestelmien välillä, tuottavat C-ITS-palveluita liikenneverkon käyttäjille sekä tarjoajat tärkeää reaaliaikaista tilannekuvaa liikenneverkon tilasta ja toiminnasta ulkopuolisille järjestelmille (mm. liikenteen ohjaus, tilannekuvajärjestelmät). IP-verkkopohjaisissa pitkän kantaman tiedonsiirtoon perustuvissa ratkaisuissa C-ITS-keskusyksiköiden rooli kasvaa merkittävästi verrattuna lyhyen kantaman tiedonsiirtoratkaisuihin. Ne muodostavat ja välittävät C-ITS-viestejä IP-verkossa toimien infran ja ajoneuvojen välisen viestinnän keskeisinä välityspisteinä. C-ITS-viestien muodostamisessa keskusyksiköt hyödyntävät joko ajoneuvoyksiköiltä, tienvarsiyksiköiltä tai C-ITS-järjestelmän ulkopuolelta saatavia lähtötietoja.

IP-verkkopohjaisissa C-ITS-järjestelmissä C-ITS-keskusyksiköt saattavat käsitellä merkittäviä määriä lähtötietoja muodostaen niiden avulla C-ITS-viestejä sekä välittävät suuria määriä viestejä alueellisten C-ITS-keskusyksiköiden ja tiedonvaihtopalvelimien välillä. Kun C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten mukainen C-ITS-keskusyksikkö muodostaa ja välittää C-ITS-viestejä, se allekirjoittaa muodostamansa viestit ja todentaa vastaanottamiensa C-ITS-viestien eheyden ja luottamuksellisuuden niiden allekirjoitusten ja lähettäjän tunnistetietojen perusteella (verifiointi). Toiminta voi edellyttää allekirjoittamista tai allekirjoitusten verifiointia merkittäville viestimäärille. Nämä tehtävät ovat keskusyksiköille raskaita kryptografisia paljon laskentatehoa vaativia tehtäviä. Tämä laskennallisesti raskas C-ITS-yksiköiden tehtävä saattaa pahimmassa tapauksessa heikentää C-ITS-palveluita tarjoavan järjestelmän suorituskykyä.

C-ITS-keskusyksiköiden operointiin ja valmistukseen liittyvät vaatimukset on määritelty aikaisemmin tässä dokumentissa luvussa 4. Luvussa 3 käsiteltiin eurooppalaisissa C-ITS-järjestelmissä käyttöönotettava yhtenäinen PKI-varmenteisiin perustuva C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS). Hallintajärjestelmä määrittelee tavat hallita, jaella ja käyttää C-ITS-viestinnän turvaamiseksi tarkoitettuja varmenteita (sertifikaatteja).

Tässä luvussa keskitytään tarkemmin C-ITS-keskusyksiköiden rooliin osana C-ITS-järjestelmää, niiden väliseen viestintään sekä viestintään liittyviin tiedon luottamuksellisuutta ja eheyttä varmistaviin allekirjoitustoimenpiteisiin. Luvussa esitellään C-Roads-yhteistyöfoorumin määrittelemän C-ITS-arkkitehtuurin mukainen C-ITS-viestinnän yleiskuvaus ja siihen liittyvät erilaiset tiedonsiirtovaihtoehdot sekä C-ITS-viestinnän tietoturvan toteuttamisperiaatteet ja arvioidaan C-ITS-viestien allekirjoittamiseksi tarvittavien toimenpiteiden vaikutuksia C-ITS-palveluiden ja C-ITS-keskusyksiköiden suorituskykyyn. Luku sisältää myös kuvitteellisen pitkän kantaman tiedonsiirtoon perustuvan esimerkin kansallisesta C-ITS-palvelutoteutusten arkkitehtuurista.

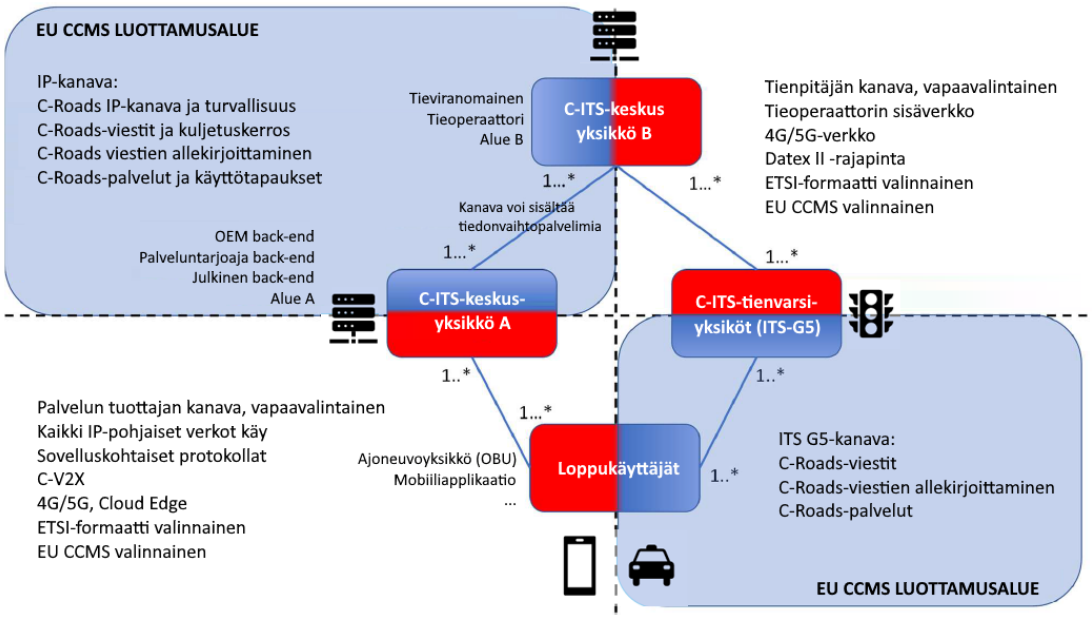
6.2 C-ITS-tiedonsiirron yleiskuvaus

6.2.1 C-ITS-tiedonsiirtoratkaisut

C-Roads-yhteistyöfoorumin tavoitteena on luoda harmonisoitu C-ITS-palvelutoteutusten tekninen arkkitehtuuri, joka mahdollistaa Euroopan sisällä yli rajojen toimivan yhdenmukaisen C-ITS-järjestelmän toiminnan. Tätä tavoitetta osaltaan tuetaan C-Roads-spesifikaatiossa C-ITS IP Based Interface Profile asetetuilla IP-pohjaisiin verkkototeutuksiin liittyvillä määrittelyillä (C-ITS IP Based Interface Profile 2024). Spesifikaatio esittelee C-ITS-tiedonsiirtoon liittyvät erilaiset vaihtoehdot sekä niiden suhteen C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) määrittelyjen mukaisten turvatunnusten käyttöön. Määritelmä sisältää tiedonsiirron yleiskuvauksen lisäksi IP-verkkoihin pohjautuvan C-ITS-palvelutoteutusten arkkitehtuurin keskeisten komponenttien, C-ITS-keskusyksiköiden sekä tiedonvaihtopalvelimien välisten yhteyksien, yhteistoiminnan ja käytettävien rajapintojen teknisen toiminnan määrittelyn, joita käsitellään laajasti tässä sekä seuraavassa selvitystyön luvussa 7.

Kuvassa 2 alla on esitetty C-Roadsin määrittelemä C-ITS-tiedonsiirron yleiskuvaus. Kuvassa esitellään C-ITS-palvelutoteutuksen arkkitehtuurin eri elementtejä sekä vaatimukset C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisen varmenteen käyttöön C-ITS-viestien allekirjoittamiseksi.

Kuvan 2 mukaisesti C-ITS-viestit allekirjoitetaan ITS-G5-tiedonsiirtotapaa hyödyntävässä tienvarsiyksikön ja ajoneuvoyksikön välisessä viestinnässä (oikea alakulma) sekä IP-verkkopohjaista tiedonsiirtoa hyödyntävässä C-ITS-keskusyksiköiden välisessä viestinnässä (vasen yläkulma). Kuvan mukaisesti C-ITS-tienvarsiyksiköiden ja tienpitäjän keskusyksikön välinen tiedonsiirtotapa on tienpitäjän vapaasti valittavissa, eikä C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen viestien allekirjoittaminen ole pakollista. C-ITS-palveluita tarjoavien keskusyksiköiden (kuvassa keskusyksikkö A) ja palveluiden loppukäyttäjien päätelaitteiden (mobiililaite tai C-ITS-ajoneuvoyksikkö) välinen kommunikointitapa on myös palveluntuottajien vapaasti valittavissa.



Kuva 2. C-Roads-spesifikaation mukainen C-ITS-tiedonsiirron yleiskuvaus (mukaillen C-ITS IP Based Interface Profile, 14).

C-Roadsin määrittelemät C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) turvatunnusten käytön vaatimukset ovat keskeisessä roolissa viestien allekirjoittamisen, C-ITS-yksiköiden sekä verkon resurssivaatimusten kanssa. Tätä aihetta käsitellään tarkemmin tämän selvitystyön luvussa 6.4. Seuraavissa alaluvuissa esitellään tarkemmin C-ITS-ratkaisujen tiedonsiirtoon käytettävät erilaiset ratkaisut.

6.2.2 Lyhyen kantaman tiedonsiirto

Lyhyen kantaman tiedonsiirtoratkaisu perustuu ITS-G5-teknologian hyödyntämiseen, joka on eurooppalainen standardi lyhyen kantaman tiedonsiirron mahdollistamiseksi ajoneuvojen sekä ajoneuvojen ja tienvarsilaitteiden välillä (kuva 2, oikea alakulma).

ITS-G5-standardi perustuu 802.11p -teknologiaan, joka on yhteistoiminnallisen liikennejärjestelmän käyttöön kehitetty IEEE:n[1] 802.11 Wi-Fi standardisarjan yksi versio. Yhdysvalloissa 802.11p -teknologiasta alettiin käyttää nimitystä DSRC (Dedicated Short-Range Communications). Euroopassa käytettiin aluksi ETSI/CEN-standardoinnin osana (v. 2010) samaa DSRC-termiä, mutta myöhemmin 2010-luvulla tekniikkaan liittyen siirryttiin käyttämään nimitystä ITS-G5. ITS-G5-tekniikan tiedonsiirtotapa (fyysinen ja siirtokerros) on määritelty standardissa ETSI EN 302 663, jonka viimeisin versio on julkaistu 1.7.2020 (versio 1.3.1).

Laajemmin C-ITS-yksiköiden lyhyen kantaman tiedonsiirtoratkaisun tekninen viitearkkitehtuuri, mm. käytetyt OSI-mallin[2] mukaiset tiedonsiirron kerrokset, tiedonsiirtorajapinnat sekä yhteentoimivuusvaatimukset määritellään ETSI EN 302 665 sekä ISO 21217 -standardeissa.

Radioteknologiaan perustuvan lyhyen kantaman tiedonsiirtoratkaisun kehittämisessä on erityisesti keskitytty ajoneuvojen väliseen viestintään. Se on optimoitu suurella nopeudella liikkuvien yksiköiden väliseen tiedonsiirtoon sekä pienen tiedonsiirtoviiveen vaatimuksiin. ETSI ITS-G5 C-ITS-yksiköt käyttävät 5,85–5,925 GHz taajuuskaistaa, jonka avulla ne pystyvät kommunikoimaan ympärisäteilevästi 300–1000 metrin säteellä lähettävästä yksiköstä. C-ITS-viestien lähetystiheys vaihtelee viestityypistä riippuen ollen tyypillisesti 0,1–10 Hz. (C-Roads WG2 Deployment Documentation 2024)

Käytettäessä ITS-G5-tiedonsiirtotapaa C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) on oleellinen osa viestien aitouden varmistamiseksi, sillä viestejä lähetetään radiotietä pitkin ”radiomajakan” tavoin (broadcast), jolloin viestejä voi vastaanottaa ja lähettää kuka tahansa tällä taajuusalueella.

---

[1] IEEE (Institute of Electrical and Electronics Engineers) on maailman suurin ammatillinen järjestö, jonka kehittämä ensimmäinen langattoman Ethernet-verkon standardi julkaistiin vuonna 1997. ITS-ympäristöön tarkoitettu versio 802.11p (Wireless Access in Vehicular Environments, WAVE) julkaistiin vuonna 2010.

[2] OSI-malli (Open Systems Interconnection) on yleinen tietoliikenneteknologiassa käytettävä referenssimalli, joka kuvaa tiedonsiirtoyhteyksien toiminnan seitsemässä eri kerroksessa. Kullakin kerroksella on oma rooli viestinnän toteutuksessa. OSI-mallin on määritellyt standardointijärjestö ITU-T (International Telecommunication Union) vuonna 1984. Jatkossa OSI-mallin kerroksiin viitataan OSI-x, jossa x viittaa OSI-mallin kerroksen numeroon.

ITS-G5-viestintää hyödynnettäessä C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen C-ITS-viestien muodostaminen ja allekirjoittaminen tapahtuu joko ajoneuvo- tai tienvarsiyksikössä. Tällöin lyhyen kantaman tiedonsiirtoon perustuvan C-ITS-järjestelmän näkökulmasta allekirjoittamisen prosessi on hajautettu suurelle määrälle C-ITS-yksiköitä. Tässä ratkaisussa C-ITS-yksiköiden koko käytettävissä oleva tiedonsiirtokaista ja laskentateho on C-ITS-palveluiden käytössä. Lyhyen kantaman tiedonsiirrossa käytettävän radioteknologian toimintasäde on kuitenkin rajallinen, jolloin tieverkon kattamiseen tarvitaan laaja tienvarsiyksiköiden verkosto. ITS-G5-viestintää käyttävissä maissa tienvarsiyksiköitä on tavallisesti tieverkolla sijoitettu yhden tai joidenkin kilometrien etäisyyksille toisistaan. Katkeamattoman kattavuuden saavuttaminen edellyttäisi tiheämpää tienvarsiyksiköiden verkostoa. Myös kaupunkiolosuhteissa tienvarsiyksiköiden etäisyydet voivat olla lyhyemmät.

Lyhyen kantaman tiedonsiirrossa käytettävän korkean taajuuden vuoksi liikennöinti on herkkä lähettäjän ja vastaanottajan välisten esteiden aiheuttamille häiriöille. Yleisesti vaatimuksena pidetään esteetöntä lähettäjän ja vastaanottajan välistä yhteyttä (”line-of-sight”-periaate)

Lyhyen kantaman tiedonsiirtoratkaisun kokonaisuuteen kuuluu myös C-ITS-tienvarsiyksiköiden ja C-ITS-keskusyksikön välinen IP-verkolla toteutettava osuus. Tämä on esitetty kuvassa 2 oikeassa yläkulmassa. Tämän osuuden tarkoitus on lyhyen kantaman tiedonsiirtoon perustuvissa C-ITS-järjestelmissä tuottaa tietoja ajoneuvojen ja liikennejärjestelmän tilasta (esim. ajoneuvojen sijainti, nopeus ja suunta, käyttäytyminen, liikenneverkon häiriötilanteet) C-ITS-keskusyksiköille. Keskusyksiköt puolestaan tarjoavat tietoa C-ITS-järjestelmän ulkopuolisten liikenteen tilannekuva-, analysointi- ja ohjausjärjestelmien käyttöön.

Ratkaisussa ajoneuvoyksiköt välittävät tietoa C-ITS-tienvarsiyksiköille ITS-G5-teknologialla. C-ITS-tienvarsiyksiköt lähettävät tiedot C-ITS-keskusyksikölle tyypillisesti suljetun ja kiinteän IP-verkon välityksellä (esim. tienpitäjän verkko).

6.2.3 Pitkän kantaman tiedonsiirto

C-ITS-järjestelmien pitkän kantaman tiedonsiirrolla tarkoitetaan C-ITS-viestien välittämistä infran ja ajoneuvojen välillä kiinteiden IP-verkkojen ja matkaviestinverkkojen avulla. Ratkaisun tavoitteena on hyödyntää matkaviestinverkkoja C-ITS-palveluiden tarjoamiseksi autoilijoille niin, että tien- ja kadunvarsia ei tarvitsisi varustaa merkittävällä määrällä C-ITS-tienvarsiyksiköitä.

Pitkän kantaman tiedonsiirtoon perustuvan ratkaisun taustalla on kaupallisten matkapuhelinverkkojen kehitys 3G-teknologian kautta huomattavasti nopeampaan ja viiveettömämpään 2010-luvulla vakiintuneeseen 4G-teknologiaan (tunnetaan myös nimellä 4G LTE, Long-Term Evolution), sekä nykyisin jo laajasti käytössä olevaan matkaviestinverkkojen viidennen sukupolven 5G-teknologiaan (tunnetaan myös nimellä 5G NR, New Radio). Uusien matkaviestinverkkojen selvästi parantunut suorituskyky sekä kapasiteetin kasvun aiheuttama viiveiden pieneneminen on luonut mahdollisuuden hyödyntää kyseisiä teknologioita tehokkaasti infran ja ajoneuvojen välisessä viestinnässä.

C-Roadsin määrittelyjen mukaisen pitkän kantaman tiedonsiirtoon perustuva järjestelmä koostuu kuvan 2 vasemman yläkulman mukaisesti C-ITS-keskusyksiköistä, jotka on liitetty toisiinsa tyypillisesti kiinteiden IP-verkkojen avulla (esim.

Internet tai muu suljettu IP-pohjainen verkkototeutus). C-Roads määrittelee C-ITS-keskusyksiköiden välisessä viestinnässä käytettävän BI-rajapinnan (Basic Interface), viestintään käytetyn AMQP-protokollan (Advanced Message Queuing Protocol), C-ITS-viestien rakenteen sekä niiden allekirjoittamisen vaatimukset (C-ITS-turvatunnusten hallintajärjestelmän mukainen). (C-ITS IP Based Interface Profile 2023)

BI-rajapinta on tarkoitettu C-ITS-ratkaisuissa taustajärjestelmien väliseen reaaliaikaiseen tiedonvaihtoon. Yhdessä AMQP-protokollan kanssa se tarjoaa harmonisoidun, avoimen ja yhteisesti määritellyn tavan toteuttaa C-ITS-keskusyksiköiden välistä viestintää. Viestinnässä hyödynnettävä AMQP-protokolla on OASIS-organisaation[1] vuonna 2012 julkaisema sovellustason protokolla (OSI-7), joka on suunniteltu tehokkaaseen viestien välittämiseen ja jonottamiseen erityisesti hajautettujen järjestelmien välillä.

C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisella viestien allekirjoittamisella taataan keskusyksiköiden välittämien viestien eheys ja viestien lähettäjän luotettavuus. Samalla laajoissa C-ITS-palvelutoteutusten arkkitehtuureissa C-ITS-keskusyksiköiden käsittelemien viestien määrä saattaa kasvaa merkittävän suureksi, jolloin viestien allekirjoittamiseen ja allekirjoitusten tarkastamiseen liittyvät toimenpiteet tuottavat C-ITS-keskusyksiköille paljon laskentatehoa vaativia toimenpiteitä. Tätä aihetta käsitellään myöhemmin selvityksen luvussa 6.4.

C-ITS-keskusyksiköillä on pitkän kantaman tiedonsiirtoon perustuvissa ratkaisuissa kolme keskeistä roolia: (1) keskusyksiköt muodostavat useiden eri tietolähteiden avulla C-ITS-viestejä, (2) keskusyksiköt välittävät viestejä eri C-ITS-yksiköiden välillä (keskusyksiköiden välinen viestintä) sekä (3) keskusyksiköt tarjoavat varsinaisia C-ITS-palveluita loppukäyttäjille.

C-ITS-viestien muodostamisessa yhtenä keskeisenä tietolähteenä tunnistetaan liikenneverkon tilasta laajasti tietoa tarjoavat kansalliset yhteyspisteet (National Access Point, NAP), jonne liikenneverkon tilasta lähetetään laajasti tienpitäjien, kuntien ja muiden merkittäviä määriä liikennetietoa omistamien yksityisten tahojen toimesta SRTI- ja RTTI-tietoja[2]. C-ITS-viestejä voidaan myös muodostaa laajasti monenlaisten muiden tietolähteiden avulla (esimerkiksi olemassa olevan liikenteen ohjausjärjestelmät, reaaliaikaiset liikenteen mittaus- ja tunnistusjärjestelmät, joukkoistamisen avulla kerätty tieto tai matkaviestinverkkopohjaista kommunikaatiota tukevien integroitujen C-ITS-ajoneuvoyksiköiden välittämät tiedot). Kansallisia yhteyspisteitä (NAP) käsitellään vielä tarkemmin luvussa 6.2.5.

---

[1] OASIS (Organization for the Advancement of Structured Information Sharing) on teollisuustoimijoista, julkisen sektorin toimijoista sekä tutkimusorganisaatioista koostuva voittoa tavoittelematon organisaatio. Organisaation kehittämä AMQP-protokolla on julkaistu myös ISO-standardina vuonna 2014 (ISO/IEC 19464 2014) sekä OASIS-organisaation julkaisemana avoimena spesifikaationa (OASIS AMQP Protocol Specification 2012).

[2] SRTI- ja RTTI-tietojen (Safety Related Traffic Information ja Real-Time Traffic Information) EU-laajuiseen tarjoamiseen liittyvät vaatimukset on määritelty alkuperäisessä ITS-direktiivissä (2010/40/EU) sekä vaatimuksia täydentävissä delegoiduissa asetuksissa (RTTI: EU/2015/962 ja EU/2022/670, SRTI: EU/886/2013). SRTI- ja RTTI-tietojen välittämisen ja kansallisten yhteyspisteiden (NAP) vaiheittaista käyttöönottoa on säädelty uudistetussa ITS-direktiivissä (EU 2023/2661 2023).

Kuvan 2 vasemman alakulman mukaisesti ajoneuvojen ja C-ITS-keskusyksiköiden väliseen viestintään hyödynnetään tyypillisesti kaupallisia matkaviestinverkkoja, kuten 4G tai 5G. Teknologioita tai verkossa käytettäviä protokollia ei kuitenkaan ole tässä tiedonsiirron osuudessa tarkemmin määritelty. C-ITS-palveluita voidaan tässä mallissa tarjota ajoneuvoille matkapuhelimiin asennettavien mobiilisovellusten tai matkaviestinverkkoihin pohjautuvaa kommunikaatiota tukevien integroitujen C-ITS-ajoneuvoyksiköiden avulla.

C-Roads-spesifikaatiot eivät ota pitkän kantaman tiedonsiirtoratkaisussa kantaa varsinaisten tietoverkkojen toteutusarkkitehtuuriin. Pitkän kantaman tiedonsiirtoon perustuvan C-ITS-järjestelmän taustapalvelut eli kansalliset ja alueelliset C-ITS-keskusyksiköt sekä kansalliset tiedonvaihtopalvelimet on mahdollista sijoittaa julkiseen avoimeen IP-verkkoon. Tämä saattaa rajoittaa C-ITS-yksiköiden välisen viestinnän palvelutasoa, sillä julkinen Internet ei takaa palvelutasoa esimerkiksi viestinnän latenssin tai yhteyden saatavuuden osalta. Julkisessa verkossa sijaitsevien solmupisteiden toimintaa on mahdollista myös häiritä esimerkiksi nykyisin yleisillä palvelunestohyökkäyksillä (distributed denial of service, DDoS).

Pitkän kantaman tiedonsiirtoon perustuvissa ratkaisuissa C-ITS-palveluiden tarjoaminen matkaviestinverkkojen avulla saattaa sisältää myös ongelmia palvelun laadussa. Vaikka matkaviestinverkkojen suorituskyky normaalitilanteissa voidaankin nähdä riittävänä suurimpaan osaan C-ITS-palveluita, matkaviestinverkko ei julkisen Internet-verkon tavoin tarjoa lupausta palvelutasosta. Toisena matkaviestinverkkoihin liittyvänä ongelmana on tuotu esille myös verkon mahdollisia katvealueita. (Kilpiö et al. 2024)

Selvitystyön myöhempään osioon (lukuun 9) sisältyy vielä tarkempi tietoverkkoratkaisujen tarkastelu.

6.2.4 Hybridikommunikaatio

Hybridikommunikaatiolla tarkoitetaan C-ITS-järjestelmien toteutustapaa, jossa yhdistyvät lyhyen ja pitkän kantaman tiedonsiirtotavat. Toteutustapa mahdollistaa yhtäaikaisesti C-ITS-palveluiden toteuttamisen IP-verkkojen, C-ITS-keskusyksiköiden ja matkaviestinverkkojen välityksellä (pitkän kantaman tiedonsiirtoratkaisu) sekä tienvarsille asennettavien radioteknologialla toimivien C-ITS-tienvarsiyksiköiden sekä ajoneuvoihin asennettavien (samaa radioteknologiaa tukevien) C-ITS-ajoneuvoyksiköiden avulla (lyhyen kantaman tiedonsiirtoratkaisu).

Hybridikommunikaatiotavan erityisiä hyötyjä on mahdollisuus käyttää eri tiedonsiirtotapoja erilaisissa C-ITS-palveluissa. Erityisen suurta reaaliaikaisuutta ja tiukkoja verkon toiminnan palvelutasovaatimuksia vaativat palvelut voitaisiin toteuttaa paikallisesti asennettavien tienvarsiyksiköiden avulla, joita tarvitsisi asentaa vain joillekin kyseisten palveluiden kannalta keskeisille alueille. Samalla laajaa maantieteellistä kattavuutta vaativat, ei niin aikakriittiset C-ITS-palvelut voitaisiin toteuttaa IP- ja matkaviestinverkkojen avulla. Ajoneuvot voivat hybriditekniikan avulla kommunikoida lyhyen kantaman tiedonsiirtoratkaisulla keskenään ja tienvarsilaitteiden kanssa sekä matkaviestinverkon välityksellä C-ITS-keskusyksiköiden kanssa.

C-Roads tunnistaa myös tämän kaltaisen hybridiratkaisun, jossa C-ITS-viestit voidaan välittää loppukäyttäjille useampia tiedonsiirtokanavia pitkin hyödyntäen ITS-

G5-teknologiaan perustuvaa lyhyen kantaman tiedonsiirtoratkaisua sekä pitkän kantaman IP-pohjaista tiedonsiirtoratkaisua (kuva 2, s. 57).

Hybriditeknologiaan perustuvaa tiedonsiirtoratkaisua on erityisesti edistänyt matkaviestinverkkoteknologioita kehittävä 3GPP[1] (Third Generation Partnership Project). Tämän kehitystyön tuloksia kutsutaan C-V2X-teknologioiksi (Cellular Vehicle-to-Anything). Nimi viittaa nimenomaan laajaan matkaviestinverkkoteknologioiden hyödyntämiseen yhteistoiminnallisten liikennejärjestelmien kaikissa viestintätapauksissa.

C-V2X-teknologiat perustuvat matkaviestinverkkoteknologiaan, joka tarjoaa ajoneuvojen sekä ajoneuvojen ja tienvarsiyksiköiden välisen suoran tiedonsiirron 5,9 GHz taajuusalueella toimivan lyhyen kantaman tiedonsiirtoratkaisun avulla. Samalla se hyödyntää kaupallista matkaviestinverkkoratkaisua pitkän kantaman tiedonsiirtoon.

Tähän mennessä 3GPP-projektissa on valmiina määriteltynä 4G-verkkoihin perustuva C-V2X tekninen spesifikaatio LTE-V2X, joka on myös integroitu ETSI-standardeihin ETSI TS 136 331 sekä ETSI TS 136 414. Siinä lyhyen kantaman tiedonsiirron rajapintaa kutsutaan PC5-rajapinnaksi (tai LTE-V2X Direct) ja pitkän kantaman tiedonsiirrossa matkaviestinverkkoa hyödyntävä viestintä käyttää Uu-rajapintaa. Tämän teknologian lyhyen kantaman tiedonsiirtoon perustuvaa versiota on pilotoitu myös Suomessa (Kynsijärvi et al. 2024).

5G-verkkoihin pohjautuvan NR-V2X-teknologian (New Radio V2X) määrittelytyö on myös jo pitkällä. Tässä teknologiassa lyhyen kantaman tiedonsiirron rajapintaa kutsutaan NR sidelink -rajapinnaksi ja pitkän kantaman tiedonsiirto toteutetaan NR Uu -rajapinnan avulla. NR-V2X on osa laajempaa 3GPP:n NR-5G määrittelytyötä (”38-sarja”, Radio technology beyond LTE). Näiden määrittely ja standardointi osaksi ETSI-standardeja on vielä kesken.

Hybridiratkaisujen yleistymisen keskeiseksi ongelmaksi nähdään tällä hetkellä perinteisen ITS-G5-teknologian ja 3GPP:n määrittelemien C-V2X-teknologioiden yhteentoimimattomuus, jolloin eri teknologioilla varustetut ajoneuvot eivät voi kommunikoida suoraan keskenään. Sama koskee myös tienvarsille asennettuja C-ITS-tienvarsiyksiköiden ja ajoneuvojen välistä viestintää.

Vuoden 2019 delegoidussa asetusehdotuksessa todettiin jo 3G- ja 4G-verkkojen sisällyttäminen todennäköisinä lisäyksinä ensisijaisten C-ITS-palveluiden tarjoamiseksi. 3GPP:n määrittelemät C-V2X-ratkaisut tunnistettiin mahdollisina teknologialisäyksinä komission asetuksiin, joskin samalla mainittiin yhteentoimivuusvaatimus olemassa olevien teknologioiden (eli ITS-G5-teknologian) kanssa (EU C/2019/1789 2019, kohta 30). C-Roads on jatkanut näiden ajatusten edistämistä oman määrittelytyön avulla.

[1] 3GPP on laaja vuonna 1998 perustettu yhteistyöprojekti, joka keskittyy erityisesti matkaviestinverkkoteknologioihin pohjautuvien teknologioiden kehittämiseen IoT-sovellusten tarpeisiin. Työhön osallistuu 7 standardointijärjestöä (mm. ETSI) sekä markkinatoimijapartnereita, kuten 5GAA (5G Automotive Association), joka yhdistää autoteollisuus-, teknologia- ja telekommunikaatiotoimijoita.

Delegoidun asetusehdotuksen jälkeen C-V2X-teknologiat ovat kehittyneet merkittävästi ja 4G-verkkoihin perustuvat versiot on integroitu osaksi ETSI-standardeja. Samalla Aasiassa ja Amerikassa on tehty jo selkeitä linjauksia C-V2X-teknologioiden hyödyntämiseen, mm. Yhdysvaltain liittovaltion viestintäkomissio FCC (The Federal Communications Commission) hyväksyi marraskuussa 2024 C-V2X-teknologian käytön 5,9 GHz taajuuskaistalla (FCC C-V2X Auto Safety Spectrum Rules 2024). Autovalmistajat ovat myös tuoneet esille selkeän kiinnostuksen erityisesti 5G-teknologioihin perustuvaa vielä kehityksen alla olevaa NR-V2X-teknologiaa kohtaan.

Samaan aikaan joissakin Euroopan maissa on jo investoitu merkittävästi ITS-G5-teknologiaan ja siihen perustuvia ekosysteemejä on syntynyt erityisesti Keski-Eurooppaan. Esimerkiksi merkittävät tieoperaattorit Autobahn (Saksa) ja Asfinag (Itävalta) ovat varustaneet moottoriteitä merkittävillä määrillä ITS-G5-tienvarsiyksiköitä (TEN-TEC EU-maiden C-ITS-keskusyksiköt 2025). Esimerkiksi Itävallan moottoriteille on asennettu vuoden 2024 loppuun mennessä yli 500 ITS-G5 tienvarsiyksikköä (keskimäärin yksi jokaista neljää kilometriä kohden). Samalla Autobahn on tienvarsiyksiköihin tehtyjen investointien lisäksi panostanut älykkäiden tietyömaatrailereiden kehitykseen ja käyttöönottoon. Vuoden 2024 loppuun mennessä tavoitteena on ollut varustaa noin 1200 kappaletta älykkäitä tietyömaatrailereita ITS-G5-teknologialla, jotka tuottavat C-ITS-viesteinä tietyömaavaroituspalveluita lähestyville ajoneuvoille. Saksalainen autovalmistaja Volkswagen on varustanut vuosien 2019–2024 aikana jo yli 1,3 miljoonaa autoa ITS-G5-tuella. (C-Roads webinar 2024)

Vaikka Euroopassa on jo yli 10 vuoden ajan kehitetty yhteiseurooppalaista C-ITS-järjestelmää, voi kahden keskeisen teknologian yhteentoimimattomuus lopulta aiheuttaa merkittäviä ongelmia C-ITS-palveluiden käyttöönotossa. Näin voi käydä, jos eri maat ja eri autonvalmistajat sitoutuvat eri teknologoihin. Samaan aikaan komissiolta on toivottu tähän aiheeseen liittyvää selkeää kannanottoa mieluiten uuden delegoidun asetuksen muodossa koskien eurooppalaisen C-ITS-järjestelmän vaatimuksia.

6.2.5 Kansallisen yhteyspisteen (NAP) hyödyntäminen

Pitkän kantaman tiedonsiirtoa käsittelevässä luvussa 6.2.3 tuotiin jo esille kansallisen yhteyspisteen (National Access Point, NAP) rooli osana C-ITS-palvelutoteutusten arkkitehtuuria. Koska tällä ratkaisulla on niin keskeinen rooli C-ITS-palveluiden toteuttamisessa, käsitellään sitä erillään vielä tässä erillisessä luvussa.

Kansallinen yhteyspiste (NAP) on C-ITS-ekosysteemistä erillään oleva kokonaisuus, jolla on laajempi rooli tieliikenteeseen liittyvien tietojen avoimessa jakelussa ja samalla ITS-toimialan ja siihen liittyvien järjestelmien kehittämisessä. Se ei itsenäisenä järjestelmänä ole siis osa C-ITS-järjestelmää, eikä sitä kohtaan kohdistu samoja vaatimuksia. Kansalliseen yhteyspisteeseen toimitettavat tietotyypit ovat kuitenkin monissa tapauksissa sellaisia, joiden avulla voidaan muodostaa C-ITS-viestejä ja siten tarjota C-ITS-palveluita. Toisaalta yhteyspisteeseen tuotettavat tiedot ovat myös sellaisia, joita C-ITS-järjestelmällä on mahdollisuus tuottaa, joten näiden kokonaisuuksien synergioita on syytä tarkastella.

Kansallisen yhteyspisteen (NAP) kehitykseen liittyvien vaatimusten taustalla on Euroopan komission pyrkimykset edistää tieliikenteen datan saatavuutta ja tiedonvaihtoa sekä turvallisuutta edistävien loppukäyttäjäpalveluiden syntymistä,

joista yhtenä esimerkkinä ovat C-ITS-palvelut. Yhteyspisteeseen välitettävien SRTI- ja RTTI-tietojen sääntelykehikko velvoittaa tienpitäjiä tuottamaan kansalliseen yhteyspisteeseen koneluettavassa muodossa välttämättömiä sääntöjä ja rajoituksia, verkon tilaa koskevia sekä turvallisuuteen liittyviä tietoja. Näihin kategorioihin kuuluvat mm. erilaiset rajoitustiedot, häiriötilanteisiin, tien tai kaistan sulkemiseen sekä sääolosuhteisiin liittyvät tiedot. Yhtäläisyyksiä C-Roads Platform -yhteistyöryhmän määrittelemiin C-ITS-palvelukategorioihin on siis selvästi. Myös kansallisen yhteyspisteen suunnitteluun ja toteutukseen liittyen on asetettu velvoitteita, joilla pyritään huomioimaan tietojen tuottamiseen liittyvät sidosryhmät sekä uudet tietolajit ominaispiirteineen. (Laine & Kotilainen 2024)

Kansalliseen yhteyspisteeseen (NAP) liikennetietoja voidaan toimittaa eri formaateissa, joita ovat pääasiassa DATEX2-, Inspire- sekä TN-ITS-formaatit. Kansalliseen yhteyspisteeseen toimitetuista tiedoista on mahdollista muodostaa keskitetysti C-ITS-viestejä. C-ITS-toteutuksissa C-ITS-keskusyksiköt voivat lukea yhteyspisteen kautta tosiaikaisia liikennejärjestelmän tilannetietoja (esimerkiksi liikennemerkkitiedot ja niiden vaikutusalueet, sääolosuhteet, häiriötilanteet tai tietyömaiden sijainti) ja muodostaa näiden avulla kuhunkin aiheeseen liittyviä C-ITS-viestejä.

Kansallisen yhteyspisteen (NAP) avulla muodostettuja C-ITS-viestejä voidaan tarjota loppukäyttäjille useilla tavoilla riippuen C-ITS-järjestelmän toteutustavasta. C-ITS-keskusyksikön muodostamia C-ITS-viestejä voidaan välittää loppukäyttäjille lyhyen kantaman tiedonsiirtoratkaisuissa välittämällä viestit aluksi IP-verkon kautta C-ITS-tienvarsiyksiköille, jotka välittävät ne lyhyen kantaman tiedonsiirrolla loppukäyttäjille. Loppukäyttäjien saavutettavuus tässä ratkaisussa on siis täysin suhteessa tienvarsiyksiköiden avulla rakennettavan verkon laajuuteen. Pitkän kantaman tiedonsiirron vaihtoehdossa viestit voidaan välittää matkaviestinverkkojen välityksellä loppukäyttäjille palveluntarjoajien kehittämien C-ITS-mobiilisovellusten avulla tai välittämällä tiedot suoraan ajoneuvojen integroituihin C-ITS-ajoneuvoyksiköihin. Ajoneuvoyksikön tulee luonnollisesti tukea näin ollen pitkän kantaman tiedonsiirron teknologioita.

Huomionarvoista kansallisen yhteyspisteen (NAP) käytössä C-ITS-viestien muodostamiseen on, että C-ITS-keskusyksiköiden operaattorit ovat vastuussa C-ITS-viestien muodostamisen yhteydessä käytettävien lähtötietojen luotettavuudesta. Tämä vastuu asetetaan C-ITS-turvallisuuspolitiikkadokumentissa, jota on käsitelty aikaisemmin tämän selvityksen luvussa 4.2 (C-ITS-yksiköiden operointi).

Tietojen ajantasaisuuden ja laadun varmistus ovatkin keskeisiä ratkaistavia asioita, jotta kansalliseen yhteyspisteeseen (NAP) kerättyjen tietojen ja sitä kautta muodostettuja C-ITS-viestejä voitaisiin pitää varteenotettavana toteutusmallina C-ITS-palveluille.

6.3 Tietoturvan toteutus

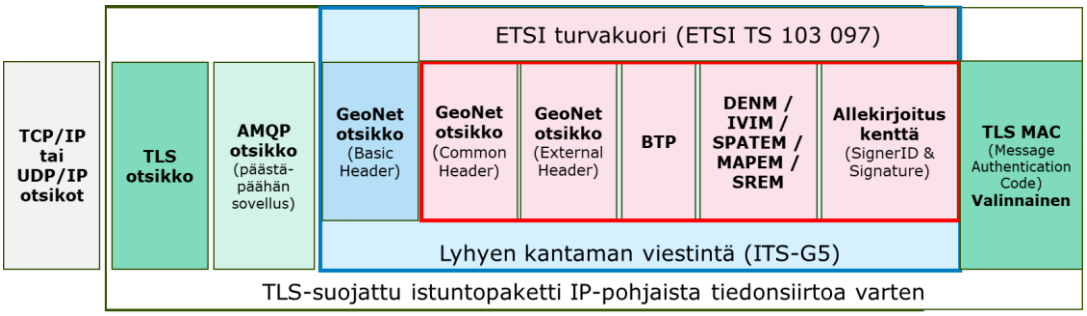
Tässä alaluvussa esitellään lyhyen ja pitkän kantaman tiedonsiirtoon liittyvät elementit, joilla varmistetaan viestien eheys ja luottamuksellisuus sekä viestinnän turvallisuuteen liitetyt elementit pitkän kantaman vaihtoehdossa. C-ITS-palvelutoteutusten arkkitehtuureissa viestinnän turvallisuuteen liittyvä C-ITS-varmennepolitiikkaan perustuva C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) ja sen toimintaperiaatteet on kuvattu erikseen jo aikaisemmin selvityksen luvussa 3. Tässä luvussa tietoturvan toteutusta avataan vielä tarkemmin viestien

rakenteiden, pitkän kantaman tiedonsiirrossa käytettävien taustajärjestelmien välisten istuntojen sekä viestien allekirjoittamisen näkökulmista.

Omassa alaluvussa esitellään C-ITS-viestin rakenne C-Roadsin teknisiin asioihin keskittyvän työryhmän II tietoturva-asioihin keskittyvän alatyöryhmän spesifikaation C-ITS Security & Governance mukaisesti (C-ITS Security & Governance 2023). Toinen alaluku esittelee C-ITS-viestien allekirjoittamisen periaatteet ja kolmannessa alaluvussa kuvataan pitkän kantaman tiedonsiirrossa taustajärjestelmien välisten istuntojen tietoturvan toteutustapa.

6.3.1 C-ITS-viestien rakenne

C-ITS-viesti on EU:n C-ITS-turvatunnusten hallintajärjestelmän mukainen tosiaikainen viesti, jota välitetään eri C-ITS-yksiköiden välillä ja se sisältää varsinaisen C-ITS-palvelun tietosisällön. Viestin sisältö eri tiedonsiirtotavoissa on esitetty alla kuvassa 3.



Kuva 3. Pitkän ja lyhyen kantaman tiedonsiirtoon soveltuvan C-ITS-viestin rakenne (mukaillen C-ITS Security & Governance 2023, 12).

Lyhyen kantaman tiedonsiirtoratkaisuun vaadittavat protokollat ja niiden otsikot on esitetty kuvan 3 sisimmässä ETSI-turvakuorta esittävässä punaisessa osuudessa sekä tämän turvakuoren ulkopuolella olevasta paketin reititykseen tarkoitetusta otsikkokentästä (GN Basic Header).

Lyhyen kantaman tiedonsiirrossa viesti sisältää seuraavat neljä eri elementtiä: (1) C-Roads-spesifikaatioiden mukainen C-ITS-viesti (DENM, IVIM jne.), (2) BTP-protokollan (Basic Transport Protocol) mukainen otsikkokenttä (OSI-4, kuljetuskerros), (3) pakettien reitityksen toteuttavat GeoNetworking-protokollan otsikkokentät (OSI-3, verkkokerros), sekä (4) viestin eheyden ja lähettäjän luottamuksellisuuden varmistamiseksi tarkoitettu allekirjoituskenttä. Kun viesti on ensin muodostettu näiden protokollakerrosten kenttien avulla, se on valmis lähetettäväksi siirtoyhteydelle (OSI-2, siirtoyhteyskerros), joka on lyhyen kantaman tiedonsiirrossa C-Roadsin mukaisesti ITS-G5.

Yllä kuvattujen C-ITS-viestin kenttien avulla varmistetaan viestien reititys sekä luottamuksellisuus ja eheys lyhyen kantaman tiedonsiirtoon perustuvissa ympäristöissä. Viesteissä käytetään C-Roadsin määrittelemiä viestityyppejä ja viestien reititys oikeille vastaanottajille sekä sovelluksille varmistetaan GeoNetworking- ja BTP-protokollien avulla. Lähettäjän luottamuksellisuus ja viestin eheys varmistetaan C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisten varmenteiden avulla toteutettavilla viestien allekirjoituksilla.

IP-verkossa toteutettava viestintä vaatii edellisten protokollien mukaisten otsikkokenttien lisäksi kyseisessä verkossa toimivia protokollia. AMQP-protokolla

(Advanced Message Queuing Protocol) esiteltiin jo aikaisemmin luvussa 6.2.3 osana pitkän kantaman tiedonsiirron esittelyä. Se on IoT-sovelluksiin erityisesti kehitetty avoin ja kevyt OSI-mallin sovellustasolla (OSI-7) toimiva protokolla. Protokollan avulla toteutetaan sovellustasolla viestien vastaanottamiseen liittyvät jonotusmekanismit sekä viestien vastaanoton varmistamiseksi käytettävät kuittaus- ja uudelleenlähetysmekanismit. Se on suunniteltu tukemaan laajoja ja hajautettuja järjestelmiä.

Pitkän kantaman tiedonsiirrossa viestijöiden väliset yhteydet salataan istuntokohtaisesti TLS-protokollan (Transport Layer Security) avulla (versio 1.3). Tämä kokonaisuus kuvataan tarkemmin alaluvussa 6.3.3. Alla olevassa taulukossa 11 on kuvattu erillisenä taulukkona tiivistetysti C-ITS-viestin otsikkokentät, niiden tarkoitus ja standardit missä ne on määritelty.

Taulukko 11. C-ITS-viesteissä käytettävien protokollien otsikkokenttien kuvaus.

Komponentti	Määritelmä	Tarkoitus	Määritetty
ETSI turvakuori (ETSI Security Envelope)			
SignerID and Signature	Tiedon lähettäjän luottamuksellisuuden ja viestin eheyden varmistus	**SignerID** on tunniste, joka yhdistää viestin lähettäjän julkiseen avaimen varmenteeseen. Sen avulla vastaanottaja voi löytää ja käyttää oikeaa julkista avainta sekä varmistaa lähettäjän luottamuksellisuuden. **Signature** on viestin kryptografinen allekirjoitus, joka varmistaa viestin eheyden. Se luodaan lähettäjän yksityisellä avaimella ja vastaanottaja voi tarkistaa viestisisällön muuttumattomuuden julkisella avaimella.	ETSI TS 103 097
DENM / IVIM / SPATEM / MAPEM…	Viestisisältö	C-ITS-viestin varsinainen informaatiosisältö.	C-Roads-profiilispesifikaatiot
BTP	Basic Transport Protocol	Kuljetuskerrosprotokolla, jota käytetään pitkän kantaman tiedonsiirrossa ajoneuvojen ja infrastruktuurin väliseen viestintään. BTP on kevyempi ja tehokkaampi vaihtoehto kuin TCP tai UDP (User Datagram Protocol). Se on suunniteltu UDP:n tavoin yhteydettömäksi, matalan latenssin ja korkean suorituskyvyn viestintään. Se toimii erityisesti yhdessä GeoNetworking-protokollan kanssa.	ETSI EN 302 636
GN Ext. Header	GeoNetworking-protokolla	GeoNetworking-protokollan laajennettu otsikkokenttä, joka tarjoaa lisätietoja viestin reitittämiseksi paikkatietopohjaisesti. Tämä otsikko sisältää lisäkenttiä ja metatietoja, joita tarvitaan viestien optimoituun reititykseen ja käsittelyyn ajoneuvojen ja infrastruktuurin välillä.	ETSI EN 302 636

Komponentti	Määritelmä	Tarkoitus	Määritetty
GN Common Header	GeoNetworking-protokolla	GeoNet Common Header on perusotsikko, joka löytyy kaikista GeoNetworking-protokollan viesteistä. Se sisältää yleiset tiedot, jotka ovat tarpeen viestin käsittelyssä ja reitityksessä. GeoNet Common Header on yhteinen osa, johon voidaan lisätä muita laajennettuja otsikoita (GeoNet Extended Headers), riippuen viestin tarpeista ja sovelluksesta.	ETSI EN 302 636
C-ITS-viesti lyhyen kantaman tiedonsiirtoa varten (ITS-G5)			
GN Basic Header	GeoNetworking-protokolla	GeoNet Basic Header on minimiosuus, joka löytyy jokaisesta GeoNetworking-viestistä. Se sisältää kriittisiä tietoja, jotka ovat tarpeen viestin perusreititystä ja käsittelyä varten. Siihen voidaan liittää muita laajennettuja otsikoita (Extended Headers), jos tarvitaan lisätietoja viestin reitittämiseksi tai käsittelemiseksi.	ETSI EN 302 636
TLS 1.3 istuntopaketti IP-pohjaista viestintää varten, TLS end-to-end			
End-to-end Application Properties	Viestinvälityspro-tokolla	AMQP (Advanced Message Queuing Protocol) on erillinen viestinvälitysprotokolla, jota voidaan käyttää erityisesti taustajärjestelmissä, mutta se ei ole osa ETSI-standardeissa käsiteltäviä C-ITS-viestinnän perusprotokollia. AMQP-protokollan rooli IP-pohjaisissa C-ITS-ratkaisuissa on kuitenkin kuvattu C-Roads C-ITS IP Based Interface Profile Version 2.0.8 dokumentissa. AMQP on avoin, vapaasti saatavilla oleva viestintäprotokolla, jota käytetään viestien välittämiseen taustajärjestelmien välillä, jotka vaativat suurta tiedonsiirron skaalautuvuutta ja luotettavuutta.	ISO/IEC 19464:2014 sekä OASIS AMQP 1.0 Specification
TLS-otsikko	Kuljetuskerroksen (OSI-4) turvallisuus	TLS Header viittaa TLS-salausprotokollan otsikkoon, jota käytetään salaamaan ETSI-turvakuoren sisällä oleva salaamaton C-ITS-viesti IP-verkoissa toteutetussa viestinnässä. C-Roads vaatii TLS-protokollan version 1.3 käyttöä. TLS tarjoaa salauksen, viestien eheyden tarkistuksen ja autentikoinnin, jota käytetään IP-verkossa palvelimien ja järjestelmien välisessä viestinnässä.	RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3
TLS MAC, valinnainen	Viestin eheyden tarkastus	Transport Layer Security Message Authentication Code. Osa TLS-protokollaa, käytetään viestin muuttumattomuuden eli eheyden tarkastamiseen viestin vastaanottajan toimesta.	

6.3.2 C-ITS-viestin allekirjoittaminen

C-ITS-viestin muodostava ja lähettävä yksikkö allekirjoittaa digitaalisesti C-ITS-viestin C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisesti käyttäen omaa salassa pidettävää yksityistä avainta. Lähettäjän muodostama allekirjoitus sijaitsee C-ITS-viestin ETSI-turvakuoren sisällä SignerID & Signature -kentässä (kuva 3). Vastaanottaja tarkistaa kentän tietojen avulla viestin lähettäjän luottamuksellisuuden ja viestin eheyden käyttäen hyväksi lähettäjän julkista avainta. Viestin sisältöä ei tässä vaiheessa salata (sisältö ei itsessään sisällä salaista tietoa), vaan allekirjoituksen avulla voidaan varmistaa, että lähettäjä on luotettu (luottamuksellisuus) ja viestin sisältöä ei ole muutettu matkalla (eheys).

Digitaalisen allekirjoituksen muodostamiseen voidaan käyttää erilaisia matemaattisia algoritmeja, joista jo vuonna 1978 esitelty RSA (Rivest-Shamir-Adleman) on luultavasti tunnetuin ja laajimmin käytetty. Se esitteli ensimmäisenä julkisesti käytäntöön otetun julkisen avaimen järjestelmään (Public Key Infrastructure, PKI) perustuvan viestien salausalgoritmin, joka perustuu suurten kokonaislukujen tekijöintiongelmaan[1]. Yksi merkittävimmistä julkisen avaimen kryptografian tarjoamista innovaatioista on digitaalinen allekirjoitus, johon liittyvä ensimmäinen standardi julkaistiin vuonna 1991 (Digital Signature Standard, DSS, ISO/IEC 9796). (Menezes, van Oorschot, Vanstone 1996, 2)

RSA on edelleen erittäin laajasti käytössä ja sitä käytetään useiden salausstandardien osana (esim. SSL-salaus, sähköinen allekirjoitus, sähköpostien salaus, VPN-verkot). Nykyään kuitenkin tehokkaammin toimivat ns. elliptisiin käyriin perustuvat ECDSA-algoritmit (Elliptic Curve Digital Signature Algorithm) ovat yleistyneet merkittävästi erityisesti sovelluksissa, joissa viestien salaukselta vaaditaan suurta nopeutta. Uudet algoritmit perustuvat matemaattisesti toisenlaisen ongelman ratkaisuun (diskreetti logaritmiongelma, ns. elliptisen käyrän kryptografia), minkä vuoksi algoritmi toimii merkittävästi lyhyemmillä salausavaimilla. Tämä puolestaan parantaa viestien käsittelynopeutta ja vähentää viivettä.

Kaikissa käytössä olevissa salausalgoritmeissa on huomioitavaa, että viestien allekirjoittaminen on matemaattisesti raskaampi toimenpide, kuin viestin aitouden ja eheyden tarkistaminen. (Menezes, van Oorschot, Vanstone 1996, 11)

Nykyisin käytössä olevia PKI-salausalgoritmeja pidetään tällä hetkellä yleisesti hyvin turvallisina. Yleisesti kuitenkin tunnistetaan, että tulevaisuuden kvanttitietokoneet uhkaavat nykyisten salausalgoritmien tuottamaa suojaa, minkä vuoksi salausalgoritmeja kehitetään jatkuvasti (Post-Quantum Cryptography, PQC). Tästä esimerkkinä on yhdysvaltalaisen standardointi- ja teknologiainstituutin NIST (National Institute of Standards and Technology) vuonna 2015 käynnistämä projekti PQC-algoritmien standardoimiseksi. Projektia toteuttaa kyseisen instituutin tietoturvayksikkö (Computer Security Resource Center, CSRC), joka on julkaissut ensimmäisiä PQC-standardeja vuoden 2024 lopulla (Federal Information Processing Standards, FIPS 203-205).

[1] Tekijöintiongelmalla tarkoitetaan yksisuuntaista funktiota, joka perustuu ajatukseen, että on helppoa kertoa kaksi suurta alkulukua keskenään, mutta erittäin vaikea purkaa niiden tulo takaisin alkulukutekijöiksi. PKI-salausta kutsutaan sen matemaattisen taustan vuoksi yleisesti myös epäsymmetriseksi salaukseksi.

Eurooppalaisen C-ITS-järjestelmän käyttämät PKI-algoritmit[1] on kuvattu Euroopan komission C-ITS-varmennepolitiikkadokumentissa (C-ITS Certificate Policy 2024, 70–73). Varmennepolitiikka sisältää käytettävien algoritmien lisäksi myös vaatimukset käytettävien avainten pituudelle sekä vaatimukset avainten säilömiselle.

C-ITS-varmennepolitiikka määrittelee, että salausavaimet tulee säilöä kryptografisiin HSM-moduuleihin (Hardware Security Module, HSM). HSM-moduulit ovat erityisesti salausavainten turvalliseen säilytykseen ja käyttöön tarkoitettuja laiteratkaisuja. HSM-moduuleja käytetään tyypillisesti korkeaa tietoturvallisuutta vaativissa sovelluksissa, kuten maksujärjestelmissä, sähköisten asiakirjojen allekirjoituksissa tai terveydenhoitojärjestelmissä. Moduulit sisältävät myös turvaominaisuuksia laitteen mahdollisia digitaalisia ja fyysisiä murtautumisyrityksiä vastaan.

Korkean suorituskyvyn HSM-moduulit ovat viestien allekirjoitustoimintaan optimoituja laitteita ja pystyvät toteuttamaan merkittävän määrän allekirjoitustoimintoja sekunnissa. Esimerkkinä voidaan mainita ranskalainen Thales, joka on yksi maailman johtavista digitaaliseen kyber- ja tietoturvallisuuden ratkaisuihin keskittyvistä yrityksistä ja jonka HSM-moduulit (Thales Luna HSM 790) pystyvät toteuttamaan nopeammin toimiviin ECDSA-algoritmeihin perustuvia PKI-allekirjoitustoimintoja 20 000 sekunnissa (eli noin 1,7 miljardia vuorokaudessa). (Thales Luna HSMs, n.d.)

C-ITS-järjestelmän päivittäiset viestimäärät voivat nousta laajoissa C-ITS-toteutuksissa useisiin miljardeihin[2]. Tämä on huomioitava järjestelmän käyttämien laitteiden viestien allekirjoitus- ja välityskyvyssä. Tämä saattaa aiheuttaa tarvetta salausavainten ja allekirjoitusten erityisille teknisille toteutuksille (esim. laskentakapasiteetin skaalaaminen tai C-ITS-palvelutoteutuksen teknisen rakenteen suunnittelu), jotta viestien allekirjoitustoiminta ei pahimmassa tapauksessa C-ITS-palvelutoteutuksen kasvaessa lamauta C-ITS-järjestelmän toimintaa.

HSM-moduulien käyttö osana C-ITS-yksiköitä perustuu Euroopan komission C-ITS-varmennepolitiikkadokumentin esittämiin vaatimuksiin. Sen mukaisesti C-ITS-yksikön tietoturvallisuuden tason arvioinnin (ISO 15408, Common Criteria) tulee sisältää avainten hallintaan tarkoitetun HSM-moduulin tietoturvallisuuden tason validointi (tämän selvitystyön luku 4.1.3). Tämä vaatimus on kuitenkin kohdistettu C-ITS-tienvarsi- ja -ajoneuvoyksiköiden tietoturvallisuuden tason arviointiin. Vastaavia määrityksiä ei ole vielä olemassa C-ITS-keskusyksiköiden valmistusta varten.

---

[1] C-ITS-järjestelmissä käytetään viestien allekirjoittamiseen nopeasti toimivia elliptisiin käyriin perustuvia ECDSA_nitP256_with_SHA 256- sekä ECDSA_brainpoolIP256r1_with_SHA 256-algoritmejä sekä ECTL-luettelon eheyden varmistamisessa edellisiä pidemmällä salausavaimella varustettua ECDSA_brainpoolip384r1_with_SHA 384 algoritmia (tarkemmin määritelty ETSI TS 103 097).

[2] Hollannin C-ITS-ekosysteemissä (tunnetaan myös työnimellä ”Talking Traffic”) kulki vuoden 2024 loppupuolella C-ITS-viestejä C-ITS-keskusyksikön kautta vuorokaudessa yli 1,5 miljardia. Järjestelmään on liitetty kiinni yli puolet maan liikennevaloristeyksistä ja sillä toteutetaan myös monipuolisesti erilaisia C-ITS-palveluita, kuten liikennevaloristeyksiin liittyvät palvelut, hälytysajoneuvojen etuus- ja lähestymisvaroituspalveluita ja tietyömaavaroituksia (Monotch haastattelu 2024).

Viestien allekirjoittamiseksi on olemassa myös palvelinten omaan laskentakapasiteettiin tai pilvipalveluihin perustuvia ratkaisuja, joissa avainten säilytys ja allekirjoitusprosessi hoidetaan ohjelmallisesti toimintaan tarkoitetuissa ohjelmistotuotteissa. Yleisesti koetaan, että HSM-moduulit ovat tietoturvallisin tapa toteuttaa PKI-avaimiin liittyviä toimintoja, kun taas palvelin- ja pilvipalvelupohjaiset ratkaisut tarjoavat suorituskyvyn osalta skaalautuvampia sekä halvempia ratkaisuja.

HSM-moduulien käyttöön liittyvä epäselvyys on aiheuttanut eriäviä mielipiteitä HSM-moduulien käytön välttämättömyydestä PKI-avainten käsittelyssä osana C-ITS-keskusyksiköiden toimintaa. Osan mielestä HSM-moduulien käyttö on välttämätöntä ja osa kokee, että korkean fyysisen tilaturvallisuuden konesaliratkaisuissa erillinen HSM-moduulien käyttö on tarpeetonta. Tämän vaatimuksen selkiyttäminen Euroopan komission toimesta olisi tärkeää, koska sillä on merkittävä vaikutus C-ITS-keskusyksiköiden laskentakapasiteetin sekä PKI-allekirjoitusten kustannusten hallintaan.

6.3.3 Istuntokohtainen tiedonsiirron salaus

C-ITS-palvelutoteutusten IP-verkossa toimivien C-ITS-keskusyksiköiden välinen viestintä on salattava istuntokohtaisesti. Tähän toimintaan liittyvät vaatimukset on määritelty IP-pohjaisen viestinnän vaatimukset kuvaavassa C-Roads-spesifikaatiossa (C-ITS IP Based Interface Profile 2023, 51–53).

Istuntokohtaisen salauksen tulee perustua Internet-verkossa yleisesti käytössä olevaan kuljetuskerroksella (OSI-4) toimivaan ja tiedonsiirron salaavaan TLS-protokollaan. TLS-protokollan ensisijainen tehtävä on toteuttaa tietoturvallinen kahden viestijän välinen yhteys.

TLS on Internet-verkkoon liittyvien standardien ja protokolliin keskittyvän avoimen IETF-järjestön (Internet Engineering Task Force) standardoima protokolla. Protokollan uusin versio 1.3 on määritelty järjestön RFC-dokumentissa 8446 vuonna 2018, jota myös C-Roads vaatii käytettäväksi (IETF RFC 8446 2018). Tunnetuimpia TLS-sovelluksia on web-selaimien tarjoama turvallinen HTTPS-yhteys, joka käyttää salauksen toteuttamiseksi TLS-teknologiaa.

C-Roads vaatii TLS-protokollan mukaisessa viestinnässä autentikointiin ja viestien salaamiseen käytettävän X.509-standardin mukaista varmennetta, joka on määritelty IETF:n RFC-dokumentissa RFC 5280 (IETF RFC 5280 2008). Varmenteiden hallinnan ja rakenteet määrittelevä X.509-standardi on osa ISO/IEC 9594 standardisarjaa (”Directory Services”), jonka mukaisia varmenteita käytetään yleisesti verkkojen turvallisuudessa sekä identiteetin ja pääsynhallinnassa ja sähköisissä allekirjoituksissa.

C-Roadsin määrittelemä pitkän kantaman tiedonsiirtoratkaisujen taustajärjestelmien tietoturvallisuuden toteutus vastaa normaalia Internet-verkossa käytettyä kahden viestijän välistä istuntopohjaista tietoturvallisuuden toteutusta. Kuten julkisessa Internet-verkossa tapahtuvassa TLS-protokollan avulla tapahtuvassa viestinnässä, osapuolten yhteydenmuodostus alkaa käytettävästä salausprotokollasta sopimisella, missä yhteydessä jaetaan salausavaimet. Autentikointi perustuu X.509-varmenteisiin, joiden avulla osapuolet ovat varmoja, että kommunikointi tapahtuu luotettavan tahon kanssa. Tämän jälkeen viestintä salataan TLS-protokollan mukaisella tavalla.

C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisessa C-ITS-järjestelmässä käytetään IP-verkon osuudella taustajärjestelmien välisissä yhteyksissä yllä kuvattua istuntopohjaista tietoturvan toteutusta. Tämän lisäksi jokainen C-ITS-keskusyksiköiden välillä lähetettävä C-ITS-viesti on allekirjoitettu käyttäen lähettäjän yksityistä avainta, minkä avulla vastaanottaja voi todentaa viestin tulevan luotettavasta lähteestä. Tämä toimenpide tehdään riippumatta siitä, lähetetäänkö viesti lyhyen kantaman tiedonsiirron mukaisessa radioverkossa vai IP-pohjaisesti pitkän kantaman tiedonsiirron mukaisessa järjestelmässä.

TLS ja X.509 antavat vahvan turvallisuuden C-ITS-keskusyksiköiden väliselle viestinnälle. Tämän lisäksi C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) PKI-arkkitehtuurin mukainen jokaisen lähetetyn viestin digitaalinen allekirjoitus varmistaa, että vaikka hyökkääjä onnistuisi pääsemään TLS-suojattuun kanavaan, se ei voi muuttaa viestejä ilman, että vastaanottaja huomaisi tämän viestin allekirjoituksen tarkastuksen yhteydessä.

6.4 C-ITS-keskusyksiköiden kuormituksen hallinta

C-ITS-keskusyksiköt joutuvat käsittelemään laajoissa C-ITS-palvelutoteutusten arkkitehtuureissa merkittäviä määriä C-ITS-viestejä. Käsittely sisältää viestien muodostamis- ja allekirjoitustoimenpiteitä sekä vastaanotettavien ja välitettävien C-ITS-viestien eheyden ja luotettavuuden tarkastuksia (allekirjoitusten tarkastus).

C-ITS-keskusyksikön käsittelemien viestien määrä kasvaa sen tarjoamien palveluiden monipuolistuessa sekä sille viestejä lähettävien C-ITS-yksiköiden määrän kasvaessa. C-ITS-allekirjoitusten aiheuttamaa kuormitusta C-ITS-keskusyksiköille voidaan käsitellä useasta eri näkökulmasta. Tässä luvussa käydään läpi tarkemmin C-ITS-keskusyksiköihin liittyvää kuormitusta ja tuodaan esille kuormituksen hallintaan liittyviä keinoja.

6.4.1 Käyttöönotettavat palvelut

Eri C-ITS-palvelut kuormittavat C-ITS-keskusyksiköitä eri tavalla, mikä johtuu sekä palveluiden että näiden toteutusten ominaisuuksista. Palveluiden erot näkyvät erityisesti eri palveluihin liittyvissä C-ITS-viestien päivitystiheyksissä. ETSI määrittelee eri C-ITS-palveluiden teknistä toimintaa kaksiosaisessa standardisarjassa ETSI EN 302 637[1].

ETSIn mukaan yksittäinen ajoneuvo voi lähettää CAM-viestejä (Cooperative Awareness Message) riippuen ajoneuvon nopeudesta 1–10 kertaa sekunnissa (ETSI EN 302 637-2 2019, 17–18). Joitakin viestejä taas lähetetään huomattavasti harvemmin. Esimerkiksi ajoneuvot lähettävät häiriötilanteista DENM-viestejä (Decentralized Environmental Notification Message) vasta, kun häiriöitä tunnistetaan. Tapahtuman havaitsemisen jälkeen ETSI ei määrittele tarkkaan viestien lähetysvälejä, vaan ne riippuvat tapahtuman luonteesta, kestosta ja vakavuudesta (ETSI EN 302 637-3 2019, 25–26).

[1] ETSI 302 637 määrittelee CAM- ja toinen osa DENM-viestipalvelut. CAM-viestit (Cooperative Awareness Message) välittävät mm. ajoneuvojen sijainti-, suunta- ja nopeustietoja. DENM-viestien (Decentralized Environmental Notification Message) avulla voidaan välittää tietoa monipuolisesti erilaisista liikenteen ja tieverkon häiriötilanteista, kuten paikallisista ajoradan liukkaista kohdista, ajoneuvojen hätäjarrutuksista tai esteistä ajoradalla.

Liikennevalot saattavat välittää lähestyville ajoneuvoille liikennevalojen tilatietoviestejä (Signal Phase and Timing, SPAT) 1–10 kertaa sekunnissa. Lähetysväliä ei ole määritelty tarkasti ETSI-standardeissa, jolloin palvelun viestien välitysnopeus riippuu tilanteesta liikennevalojen ohjauskojeen konfiguroinneista.

Käyttöönotettavilla palveluilla ja niiden toteutustavoilla on siis merkittävä vaikutus siihen, kuinka paljon C-ITS-palvelutoteutuksissa liikkuu viestejä.

6.4.2 Käyttäjien määrä

Mitä enemmän C-ITS-palvelut saavat käyttäjiä, sitä enemmän verkossa liikkuu C-ITS-viestejä. Ensi vaiheen pitkän kantaman tiedonsiirtoratkaisuissa viestien suunta on pääasiassa C-ITS-keskusyksiköiltä loppuasiakkaille, jotka käyttävät palveluita mobiililaitteisiin asennettavien sovellusten avulla. Ajoneuvot eivät siis tuota lainkaan CAM- tai DENM-viestejä, vaan kaikki palveluviestit muodostetaan C-ITS-keskusyksiköissä, jotka tarjoavat palveluita loppuasiakkaiden matkapuhelimeen asennettuihin mobiilisovelluksiin.

Myöhemmin, kun ajoneuvojen C-ITS-ajoneuvoyksiköt lisääntyvät, niin ne voivat tuottaa merkittäviä määriä tietoja (CAM/DENM), vaihtaa näitä tietoja keskenään sekä voivat lähettää samoja tietoja keskusyksiköiden suuntaan. C-ITS-keskusyksiköissä näitä viestejä voidaan välittää ajoneuvoille sekä myös C-ITS-palvelutoteutusten ulkopuolisten järjestelmien hyödynnettäväksi.

On myös hyvä huomioida, että C-ITS-palveluiden toteutustapa vaikuttaa merkittävästi tulevaisuudessa ajoneuvojen CAM- ja DENM-viestien kulkureittiin.

Mikäli C-ITS-palvelut on toteutettu pelkästään pitkän kantaman tiedonsiirtoratkaisulla ja integroidut C-ITS-ajoneuvoyksiköt on otettu käyttöön ajoneuvoissa, voivat CAM- ja DENM-viestit siirtyä ensisijaisesti vain autonvalmistajien C-ITS-keskusyksiköihin matkaviestinverkkojen välityksellä. Mikäli C-ITS-palvelutoteutuksen arkkitehtuuri toteutetaan hybridi- tai lyhyen kantaman tiedonsiirtoratkaisulla, niin CAM- ja DENM-viestit voivat siirtyä myös lyhyen kantaman tiedonsiirron avulla C-ITS-tienvarsiyksiköille ja sitä kautta esimerkiksi kansalliselle C-ITS-keskusyksikölle. Hybridiratkaisussa ajoneuvojen muodostamat ja eteenpäin välittämät viestit on mahdollista lähettää sekä autonvalmistajalle matkaviestinverkon välityksellä että C-ITS-tienvarsiyksiköiden kautta kansalliselle C-ITS-keskusyksikölle.

6.4.3 C-ITS-palvelutoteutusten arkkitehtuurin rakenne

C-ITS-palvelutoteutusten arkkitehtuurinen toteutustapa vaikuttaa merkittävästi keskusyksiköiden toteuttamiin allekirjoitustapahtumiin. Kansallinen C-ITS-palvelutoteutus voi perustua yhteen keskitettyyn C-ITS-keskusyksikköön, jolloin kaikki infran ja ajoneuvojen väliset viestit kulkevat sen kautta.

Toisaalta keskusyksiköitä voidaan toteuttaa enemmän, jolloin allekirjoitustapahtumatkin jakaantuvat. Esimerkiksi päätieverkon palveluille yksi ja kutakin isompaa kaupunkia varten yksi. Pienemmät kaupungit voisivat toteuttaa oman C-ITS-viestinnän yhteisellä keskusyksikköhankinnalla tai käyttämällä jonkin jo olemassa olevan C-ITS-keskusyksikön tarjoamia palveluita.

Toisaalta C-ITS-keskusyksiköiden roolit voisivat jakaantua myös toteutettavien palveluiden mukaisesti. Joitakin peruspalveluita voitaisiin toteuttaa yhdestä kansallisesta keskusyksiköstä ja kaupunkikohtaisia palveluita voidaan toteuttaa

kaupunkien omien keskusyksiköiden avulla. Keskusyksiköitä voisi roolittaa myös eri tehtäviin: C-ITS-viestien muodostaminen C-ITS-palvelutoteutuksen arkkitehtuurin ulkopuolelta saatavien lähtötietojen avulla, C-ITS-viestien välittäminen alueellisten C-ITS-palvelutoteutusten välillä ja C-ITS-loppukäyttäjäpalveluiden tarjoaminen.

6.4.4 Allekirjoituspisteiden hallinta

C-ITS-palvelutoteutuksen arkkitehtuuriin liittyvillä rakenteellisilla toimilla voidaan myös hallita C-ITS-viestien allekirjoitusten suorituspaikkaa. Mikäli halutaan vähentää C-ITS-keskusyksiköiden allekirjoitustoimenpiteitä, niin useita palveluita voidaan toteuttaa erillisten C-ITS-viestien allekirjoitukseen kykenevien C-ITS-ajoneuvoyksiköiden tai tienvarsilaitteiden avulla (hybridikommunikaatiota tukevat yksiköt). Esimerkiksi rajattuja ajoneuvoryhmiä voidaan varustaa erikseen asennetuilla ajoneuvoyksiköillä (hälytysajoneuvot, julkinen liikenne), jolloin C-ITS-ajoneuvoyksiköt voivat toimia C-ITS-viestien allekirjoittajina. Samoin esimerkiksi voitaisiin vaatia, että tietyömaat varustetaan C-ITS-tienvarsiyksiköillä, jolloin tietyömailta pystyttäisiin välittämään jo valmiiksi allekirjoitettuja tietyömaiden varoitusviestejä keskusyksikölle.

Kuten aikaisemmin C-ITS-viestien allekirjoittamista käsittelevässä luvussa 6.3.2 todettiin, niin C-ITS-viestien vastaanottoon liittyvä tarkastustoimenpide on laskennallisesti vähemmän kuormittava toimenpide kuin C-ITS-viestien muodostaminen ja siihen liittyvä viestin allekirjoitusprosessi. Täten allekirjoituspisteiden hallinnalla voidaan vaikuttaa myös C-ITS-keskusyksiköiden kuormittumiseen.

6.4.5 Allekirjoitusten määrä ja keskusyksiköiden kuormitus

Kuten yllä esitetyistä (luvut 6.4.1–6.4.4) C-ITS-palveluiden arkkitehtuureihin liittyvistä ratkaisuvaihtoehdoista voi päätellä, niin C-ITS-viestien allekirjoitustapahtumien keskusyksikkökohtaista määrää voidaan hallita monenlaisilla keinoilla. Tämän vuoksi yksittäisen C-ITS-keskusyksikön toteuttamien allekirjoitusten määrä on hyvin vahvasti sidonnainen käyttöönotettaviin palveluihin, käyttäjämääriin sekä C-ITS-palveluiden arkkitehtuurin tekniseen toteutustapaan ja kansallisiin vaatimuksiin, kuten tietojen välitys C-ITS-ajoneuvo- tai tienvarsiyksiköiden avulla tai esimerkiksi kansallisen yhteyspisteen (NAP) tietosisältöjä hyödyntäen.

Keskusyksiköiden viestimääräistä kuormitusta on yllä olevan näkökulman vuoksi erilaisissa tilanteissa erittäin hankalaa arvioida. Paras vertailukohta verkossa käsiteltävien viestien määrälle on hollantilainen C-ITS-ekosysteemi. Ekosysteemi perustuu yhteen infran ja ajoneuvojen välisiä viestejä välittävään kansalliseen C-ITS-keskusyksikköön, joka käsittelee tällä hetkellä yli 1,5 miljardia viestiä päivässä. Loppuasiakkaat käyttävät C-ITS-palveluita yksityissektorin palveluntarjoajien toteuttamien C-ITS-keskusyksiköiden ja mobiilisovellusten avulla. Hollannin ekosysteemissä toteutetaan myös ammattiliikenteelle palveluita, kuten hälytysajoneuvojen priorisointia liikennevalo-ohjatuissa risteyksissä ja tietyömaista varoittavia palveluita. Hollannissa on yli puolet (n. 1500) liikennevaloristeystä kytketty kiinni järjestelmään.

Hollannin esimerkki on hyvä vertailukohta suomalaiselle tulevaisuuden C-ITS-ekosysteemille, sillä liikennevalojen määrä on maissa suunnilleen sama ja Suomessakin palvelut tullaan todennäköisesti toteuttamaan merkittäviltä osin pitkän kantaman tiedonsiirtoratkaisuilla. Toisaalta Hollannin vertailukohtaa voi

ensisijaisesti arvioida siinä kulkevien viestimäärien osalta. Hollannin C-ITS-järjestelmän kehitys on aloitettu vuonna 2016 Talking Traffic -kehitysprojektissa, jossa on kehitetty omia kansallisia teknisiä toteutustapoja. Esimerkiksi keskusyksiköt eivät Hollannin mallissa allekirjoita viestejä C-Roadsin ja C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisilla tavoilla, joihin Suomi on lähtökohtaisesti sitoutunut.

6.4.6 C-ITS-keskusyksiköiden kuorman hallinta

Tässä alaluvussa käsitellään C-ITS-keskusyksiköiden kuorman hallintaan käytössä olevia keinoja ja arvioidaan C-ITS-palvelutoteutusten tuottamaa kuormaa ja sen mahdollista hallintaa keskusyksikön kannalta.

Arvioidaan karkeasti aluksi minkälaista kuormaa C-ITS-järjestelmä voisi tuottaa sen keskusyksiköille sekä viestimäärien ja toisaalta niiden aiheuttaman tietoliikennekuorman näkökulmasta.

Viestimäärä ja PKI-operaatiot

Hollannin tämänhetkisen C-ITS-toteutuksen laajuus voisi edustaa suomalaisen C-ITS-järjestelmän laajuutta ja tasoa muutaman vuoden päästä. Todennäköisesti tämä olisi todennäköistä noin vuonna 2030, mikäli C-ITS-järjestelmä toteutetaan C-Roadsin vaatimusten mukaisesti. Oletetaan, että suomalainen C-ITS-järjestelmä perustuisi Hollannin tapaan suurelta osin yhteen kansalliseen C-ITS-keskusyksikköön ja kaikki PKI-toiminnot toteutettaisiin erillisissä HSM-moduuleissa. Tällä hetkellä markkinoilla olevat HSM-moduulit voisivat hoitaa C-ITS-viestien aiheuttaman allekirjoituskuorman (luvussa 6.3.2 mainittu referenssilaitteen suorituskyky on noin 1,7 miljardia PKI-allekirjoitusta päivässä, 20 000 operaatiota sekunnissa). Luultavasti HSM-moduuleita tarvittaisiin kaksi, koska C-ITS-viestien määrä vaihtelee liikennemäärän mukaisesti eli on päivisin suurempi kuin hiljaisina yöaikoina. Kahdentaminen olisi järkevää myös järjestelmän riskien hallinnan kannalta.

C-Roadsin määritykset keskusyksiköiden PKI-allekirjoitusten käsittelyn suhteen ovat vielä kesken, joten HSM-moduulin vaatimuksesta osana keskusyksiköiden toteutusta ei vielä tiedetä. Mikäli allekirjoitukset toteutettaisiin palvelimien omaan laskentatehoon tai HSM-pilvipalveluihin perustuen, kapasiteetti riittäisi kyseisen viestikuorman hoitamiseen vielä paremmin.

Tarvittava tietoliikennekapasiteetti

Viestiliikenteen aiheuttaman kuorman suuruutta C-ITS-keskusyksikölle voi olla hyvä arvioida myös perinteisellä tietoliikennekapasiteetin käytöllä. Alla oleva laskenta perustuu ajatukseen, että kaikki viestiliikenne reitittyy yhden pisteen kautta ja arvioon C-Roadsin mukaisen keskimääräisen verkossa kulkevan C-ITS-paketin kokoon 500–800 tavua.

C-ITS-paketin kokoarvio perustuu aikaisemmin Suomessa tehtyyn pilottiprojektiin, jossa lyhyen kantaman tiedonsiirtoratkaisussa allekirjoitetun SPAT-viestin koko oli 509 tavua (Kynsijärvi et al. 2024, 46). Tähän on lisätty pitkän kantaman tiedonsiirron IP-verkossa käytettävien protokollien otsikot (AMQP, TLS 1.3, TCP ja IP), arviolta yhteensä n. 140–280 tavua. Laskennassa käytetään 800 tavun pakettikokoa. Viestien koko voi vaihdella viestityypistä riippuen paljonkin.

Laskennan toiseksi taustaksi otetaan aikaisemmin esitetty Hollannin referenssijärjestelmä, jossa kansallinen keskitetty keskusyksikkö käsittelee tällä hetkellä vuorokausitasolla yli 1,5 miljardia viestiä. Käytetään laskennassa tähän nähden hieman reilumpaa viestimäärää eli kahta miljardia viestiä vuorokaudessa.

Yllä esitettyihin lähtöoletuksiin perustuva C-ITS-keskusyksikön käyttöön tarvittava tietoliikennekapasiteetti olisi noin 150 Mbit/s[1] suuntaansa. Kun otetaan huomioon eri vuorokauden aikojen liikennemäärän vaihtelu ja sen vaikutus C-ITS-pakettien määrään, voidaan arvioida, että keskusyksikön tarvitsema tietoliikennekapasiteetin tarve (sisään/ulos) vaihtelisi n. 50–300 Mbit/s (allekirjoituksen tuottama kuorma on tästä noin 15 %, n. 80–140 tavua per viesti).

Johtopäätöksenä voidaan todeta, että tämä on merkittävä määrä liikennettä, mutta ei kuitenkaan varsinaisia erityisjärjestelyjä vaativa. Tulos indikoi laskennan reunaehtoihin perustuvaa C-ITS-keskusyksikön vaatimaa tietoliikennekapasiteettia (esim. pilvipalveluun tarvittava kaista, johon C-ITS-keskusyksikkö sijoitetaan).

Tietojenkäsittelykapasiteetin hallinta

Allekirjoitustoimintojen tuottamaa kuormaa C-ITS-keskusyksiköillä voidaan hallita useilla eri tavoilla. Yhtenä tapana on jo aikaisemmin esille tullut C-ITS-palveluiden arkkitehtuurin suunnittelu, joka antaa paljon vaihtoehtoja C-ITS-keskusyksiköiden kuormituksen hallintaan. Tätä tapaa voi pitää perinteisenä tietojenkäsittelykapasiteetin horisontaalisena skaalauksena, jossa palvelimia lisätään järjestelmään verkon rakenteellisen kehityksen ja keskusyksiköiden roolitusten avulla. Samaa skaalauksen tapaa edustaa myös yksittäisten palvelimien kahdentaminen ja kuormantasaus.

Toinen tapa toteuttaa kapasiteetin skaalausta keskusyksiköissä on vertikaalisen skaalauksen periaatteiden mukainen yksittäisen palvelimen kapasiteetin lisäys (muisti, prosessoriteho jne.). Tälle skaalaukselle parhaat edellytykset tarjoavat pilvipalvelutoimittajat, jotka pystyvät tarjoamaan vertikaalisen skaalauksen palveluita jopa dynaamisina, jolloin kapasiteettia voidaan hallita tarpeen mukaan.

6.4.7 Johtopäätökset

Huolimatta C-ITS-palvelutoteutuksen arkkitehtuurin rakenteellisesta toteutustavasta, C-ITS-keskusyksiköt joutuvat käsittelemään merkittäviä määriä C-ITS-viestejä. Viestien määrä kasvaa, kun palveluiden ja käyttäjien määrä lisääntyy sekä ajoneuvojen sisälle asennettavien integroitujen C-ITS-ajoneuvoyksiköiden määrä kasvaa.

[1] Laskennan tavoitteena on saada tietoliikennekapasiteettitarve X Mbit/s. Vuorokaudessa keskitetyn pisteen ohittaa 2 000 000 000 kpl 0,8 kilotavun pakettia → 1 600 000 000 kilotavua. Tämä kerrottuna kahdeksalla saadaan kilobittien määrä: 12 800 000 000 Kbit = 12 800 000 Mbit. Vuorokaudessa on sekunteja 86 400 (60*60*24). Tarvittava kapasiteetti on 12 800 000 Mbit / 86 400 s = 148,15 Mbit/s.

Luvussa käytettiin tulevan suomalaisen C-ITS-järjestelmän laajuuden arvioinnissa vertailupohjana hollantilaista C-ITS-ekosysteemiä, jossa liikkuu tällä hetkellä kansallisesti yli 1,5 miljardia viestiä vuorokaudessa. Kuormituslaskennan lähtötietona käytettiin kahta miljardia C-ITS-viestiä vuorokaudessa ja arviota 800 tavun keskimääräisestä C-ITS-viestin koosta. Tämän arvioidaan olevan mahdollinen suomalaisen C-ITS-järjestelmän tilanne 2030-luvun alussa.

Lähtöoletuksiin perustuvien laskelmien perusteella viestimäärä vastaisi n. 150 Mbit/s kapasiteettitarvetta. Eri vuorokauden aikojen liikennemäärä huomioiden kapasiteettitarpeen arvioidaan vaihtelevan n. 50–300 Mbit/s.

Mikäli kansallinen arkkitehtuuri perustuu yhteen keskitettyyn C-ITS-keskusyksikköön, niin yllä kuvattu on kyseistä keskusyksikköä varten vaadittava kaksisuuntainen esimerkiksi pilvipalvelu- tai palvelinsalitoimittajalta ostettava tietoliikennekapasiteetti. Erityishuomiona sanottakoon, että tämä kapasiteettitarve ei siis viittaa yleisesti C-ITS-palvelutoteutuksen hyödyntämien tietoliikenneverkkojen kapasiteettitarpeeseen, vaan ainoastaan C-ITS-keskusyksikön vaatimaan kapasiteettitarpeeseen. Tietoliikennekapasiteetin tarpeesta johtopäätöksenä todettiin, että kapasiteetin tarve voi olla merkittävä, mutta tämä ei tuota ongelmia tietoliikenneyhteyksien tai palvelinten yleisen suorituskyvyn kannalta.

Luvussa 6.3.2 arvioitiin myös C-ITS-viestien allekirjoitustoiminnan aiheuttamaa kuormaa C-ITS-keskusyksikölle yhden kansallisen keskitetyn keskusyksikön arkkitehtuurissa. Päätelmässä todettiin, että laskentaskenaariossa käytettävien viestien (2 miljardia viestiä vuorokaudessa) allekirjoittaminen pystyttäisiin hoitamaan kahdella nykyaikaisella HSM-yksiköllä. Päätelmässä referenssinä käytettiin Thales Luna S790 HSM-moduulia (Thales Luna HSMs, n.d.), joka pystyy toteuttamaan n. 20 000 allekirjoitustoimintoa sekunnissa C-Roadsin määrittelemillä PKI-algoritmeilla (ECDSA ja allekirjoitukseen käytettävä 256-bittinen RSA-avain). Tämä tarkoittaisi keskimäärin noin 1,7 miljardia allekirjoitustapahtumaa vuorokaudessa.

Mikäli C-Roads-profiilispesifikaatiot tai C-ITS-turvallisuus- ja varmennepolitiikka eivät edellytä laitepohjaisen HSM-yksikön käyttöä, voidaan arvioitu määrä viestien allekirjoitustapahtumia toteuttaa pilvipalvelutoimittajien HSM-palveluiden tai palvelinpohjaisten ohjelmistoratkaisuiden avulla.

Allekirjoitusvaatimusten kuormittuvuudesta todettiin, että vaikka pitkän kantaman tiedonsiirtoratkaisussa ja erityisesti keskitettyyn kansalliseen C-ITS-keskusyksikköön perustuvassa mallissa viestimäärät kasvavat merkittävästi, niin tulevaisuuteen sijoittuvan skenaarion mukaisten viestimäärien allekirjoittaminen olisi toteutettavissa järkevillä kustannuksilla jo tämän päivän teknologioilla.

Kun otetaan huomioon C-ITS-palvelutoteutusten laajentuminen eli viestimäärien jatkuva kasvu, toisaalta teknologian ja laskentakapasiteettien jatkuva kehitys sekä monet muut tässäkin luvussa esitetyt tekniset ja C-ITS-palvelutoteutuksiin liittyvät arkkitehtuuriset tavat vaikuttaa C-ITS-keskusyksiköiden kuormitukseen, voidaan todeta, että pitkän kantaman tiedonsiirtoon perustuvilla C-ITS-keskusyksiköillä on hyvät edellytykset selvitä niihin kohdistuvasta kuormituksesta.

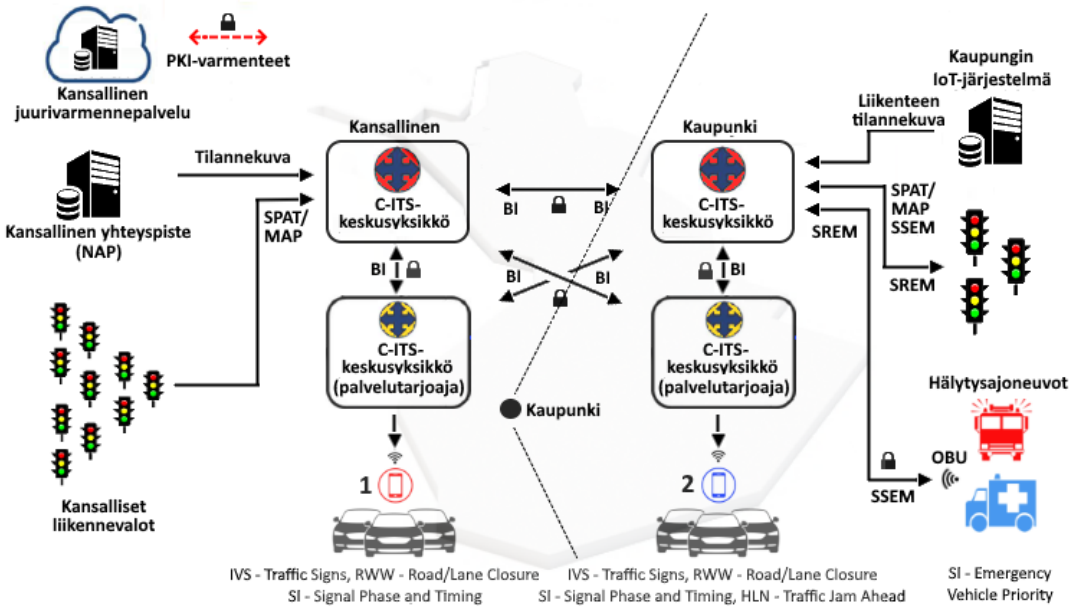
Arvio tietoliikennekaistan riittävyydestä C-ITS-keskusyksikkötoteutuksessa ei ota kantaa laajemmin ilman palvelutasotakuita toimivien julkisten tietoliikenneverkkojen soveltuvuudesta pitkän kantaman tiedonsiirtoratkaisuissa. Tätä näkökulmaa pohditaan vielä erikseen tämän selvitystyön luvussa 9.

6.5 Kansallisen C-ITS-järjestelmän esimerkkitoteutus

Tässä luvussa avataan aikaisemmin esitettyjen vaatimusten ja C-Roads-arkkitehtuurin mukainen kuvitteellinen kansallinen C-ITS-järjestelmän esimerkki. Esimerkki ei ole suositus C-ITS-järjestelmän kansallisesta toteutuksesta, vaan kuvaa mahdollista C-ITS-palveluiden toteuttamiseen käytettävää arkkitehtuuria, havainnollistaa C-ITS-keskusyksiköiden toimintaa ja C-ITS-palveluiden loppuasiakasrajapintoja, ajoneuvojen roolia sekä erilaisten lähtötietokanavien käyttöä.

Kuva 4 esittää kuvitteellisen esimerkin kansallisesta C-ITS-palvelutoteutuksen arkkitehtuurista, joka toimii yhden kansallisen C-ITS-keskusyksikön avulla, ja tämän lisäksi yksi kaupunki on ottanut käyttöön oman kaupunkikohtaisen C-ITS-keskusyksikön. Näiden kahden keskusyksikön roolina esimerkissä on toimia C-ITS-viestien muodostajina erinäisten lähtötietojen perusteella. Kummassakin C-ITS-palvelutoteutuksessa loppukäyttäjien palvelut toteutetaan palvelutoimittajien toteuttamien C-ITS-keskusyksiköiden ja mobiilisovellusten avulla (palveluntarjoajan keskusyksikön ja mobiilisovelluksen välissä käytetään palveluntarjoajakohtaisia protokollatoteutuksia, ks. kuva 2, s. 57).

Esimerkkiratkaisu on luvun 6.2.3 pitkän kantaman tiedonsiirtoratkaisun periaatteiden mukainen. Tekninen esimerkkitoteutus ei hyödynnä toiminnassaan lainkaan C-ITS-tienvarsiyksiköitä, eikä loppukäyttäjäpalveluiden tuottaminen perustu ajoneuvoihin asennettuihin C-ITS-ajoneuvoyksiköihin. Kaupunkikohtainen hälytysajoneuvojen liikennevaloristeysten etuuspalvelu on esimerkissä toteutettu ajoneuvoihin asennettujen matkaviestinverkon teknologiaa tukevien C-ITS-ajoneuvoyksiköiden (OBU) avulla. Kuvassa näkyvien C-ITS-keskusyksiköiden välisten yhteyksien avulla kaupungin C-ITS-palvelutoteutus voi hyödyntää kansallisen keskusyksikön tarjoamia palveluita (ja toisinpäin). Esimerkissä C-ITS-keskusyksiköt keskustelevat keskenään C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) periaatteiden mukaisesti ja jakelevat toisilleen tarjolla olevia C-ITS-viestityyppejä. Esimerkkiratkaisussa ei oteta kantaa, kuinka C-ITS-keskusyksiköt tai loppukäyttäjien mobiilisovellukset on toteutettu (julkinen vai yksityinen taho).



Kuva 4. Kuvitteellinen esimerkki suomalaisesta pitkän kantaman tiedonsiirtoratkaisuun ja C-ITS-keskusyksiköihin perustuvasta C-ITS-järjestelmästä.

Kansallinen C-ITS-keskusyksikkö tarjoaa esimerkkitoteutuksessa seuraavia C-ITS-palveluita tieverkon käyttäjille.

(1) Keskusyksikkö hakee kansallisen yhteyspisteen (NAP) kautta kiinteiden ja dynaamisten liikennemerkkien tilatiedot ja vaikutusalueet, joiden perusteella se tarjoaa liikennemerkkien asettaman kulloinkin voimassa olevan tilan välittävää C-Roadsin mukaista Traffic Signs IVS-palvelua (In-Vehicle Signage) omassa mobiilisovelluksessaan (C-ITS-sovellus 1).

(2) Samasta lähteestä kansallinen keskusyksikkö saa myös SRTI- ja RTTI-asetusten voimaantulon ja kansallisen yhteyspisteen (NAP) kehitystyön myötä kansallisesti tietyömaiden sijaintitiedot, joiden perusteella kansallinen keskusyksikkö muodostaa tietyömaiden varoitusviestit ja tarjoaa myös C-ITS-varoitusviestejä tietyömaita lähestyttäessä (Road Works Warning – Road/Lane Closure -palvelu).

(3) Kansalliseen C-ITS-keskusyksikköön on myös esimerkissä liitetty laajasti Fintraffic Tie Oy:n ja kaupunkien omistamia liikennevalojen ohjauskojeita, jotka tuottavat keskusyksikölle risteysten valoryhmien tilatietoja sekä aikaennusteita tilan seuraavasta vaihdosta (SPAT, MAP). Näiden perusteella C-ITS-keskusyksikkö tarjoaa tiellä liikkujille SI-palvelukategoriaan (Signalized Intersection) kuuluvaa Signal Phase and Timing -palvelua.

Esimerkissä kaupunkikohtainen C-ITS-keskusyksikkö tarjoaa kaupungin alueella liikkuville monipuolisempia C-ITS-palveluita kuin kansallinen yksikkö. Tämä on esimerkissä toteutettu kaupungeissa jatkuvasti yleistyvien Smart City IoT -ratkaisujen avulla. IoT-ratkaisu tuottaa kaupunkiliikenteestä reaaliaikaista liikenteen tilannekuvaa, jonka avulla esimerkissä tuotetaan kaupunkialueella liikkuville autoilijoille ruuhkavaroituspalvelua (Traffic Jam Ahead). Esimerkissä hälytysajoneuvojen liikennevaloetuudet on toteutettu erillisten hälytysajoneuvoihin asennettujen C-ITS-ajoneuvoyksiköiden (OBU) avulla. Etuuspalvelussa ajoneuvoyksiköt välittävät etuuspyyntöjä (Signal Request Extension Message, SREM) kaupungin operoiman C-ITS-keskusyksikön kautta liikennevaloille, jotka kuittaavat pyynnöt statusviesteillä (Signal request Status Extension Message, SSEM).

C-ITS-keskusyksiköiden välisten yhteyksien avulla esimerkissä kaupungin C-ITS-mobiilisovellus 2 voi tarjota samat kansalliset palvelut kuin mobiilisovellus 1. Se tarjoaa kaupungin alueen sisä- ja ulkopuolella kaikki kansallisesti toteutetut palvelut, mutta kaupunkialueella myös jo yllä mainittua liikenneruuhkista varoittavaa HLN-palvelukategoriaan (Hazardous Location Notification) kuuluvaa liikenneruuhkien varoituspalvelua (Traffic Jam Ahead). Kansallinen C-ITS-keskusyksikkö voisi välittää kaupunkialueella varoitusviestit lähestyvistä jononpäistä mobiilisovellukseen 1. Esimerkissä C-ITS-sovellukseen 1 ei kuitenkaan ole toteutettu kyseisen (Traffic Jam Ahead) palvelun tukea.

Edellä kuvattu mobiilisovelluksiin liittyvä esimerkki osoittaa, että C-ITS-palveluiden tuottaja itse päättää, mitkä palvelut se toteuttaa omaan sovellukseensa. Tämä koskee mobiilisovellusten lisäksi myös ajoneuvoihin integroituja C-ITS-ajoneuvoyksiköitä. Sama asia koskee myös C-ITS-palveluiden varsinaista toteutustapaa eli loppukäyttäjälle esitettävää palvelun visuaalista toteutusta. C-Roads ei määrittele vaatimuksissaan toteutukseen liittyviä tämän tason yksityiskohtia. C-Roads määrittelee omassa spesifikaatiossaan C-ITS-viestit, joiden avulla palvelut toteutetaan (C-Roads C-ITS Message Profiles 2023) sekä C-ITS-palveluiden

toteutuksen käyttötapausesimerkkien avulla omassa C-Roads-spesifikaatiossa (C-Roads C-ITS Service and Use Case Definitions 2024).

Esimerkin mukainen hälytysajoneuvoille tarjottu liikennevaloetuus perustuu ajoneuvoihin asennettuihin hybriditeknologiaa tukeviin C-ITS-ajoneuvoyksiköihin (erillisasennus). Kuvan 4 mukaisesti yksiköt pyytävät valoetuuksia matkaviestinverkon välityksellä kaupungin järjestelmään liitetyiltä liikennevalojen ohjauskojeilta C-Roadsin määrittelemien ja allekirjoitettujen etuuspyyntöviestien avulla (Signal Request Extented Message, SREM), joihin ohjauskojeet vastaavat pyynnön mahdollisesta onnistumisesta (Signal request Status Extended Message, SSEM).

Kuvan 4 mukainen kansallinen toteutusesimerkki on C-Roadsin määrittelemän arkkitehtuurin mukaisesti toteutettu. Esimerkissä C-ITS-keskusyksiköt sekä hälytysajoneuvojen C-ITS-ajoneuvoyksiköt hakevat viestien allekirjoittamiseen tarvittavat PKI-avaimet kansallisesta juurivarmennepalvelusta. Näiden avulla C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen luottamusalue toimii lukoilla kuvatuilla väleillä eli C-ITS-keskusyksiköiden sekä kaupungin C-ITS-keskusyksikön ja kaupungin hälytysajoneuvojen välisillä linkeillä. Muilla kuvan 4 mukaisilla linkeillä, kuten C-ITS-keskusyksiköiden ulkoisten lähtötietojen hakeminen (NAP, City IoT-järjestelmä) ja C-ITS-keskusyksiköiden ja mobiilisovellusten välinen tiedonsiirto ei ole C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisesti toteutettu. Näillä väleillä keskusyksiköiden operaattorit huolehtivat itse ratkaisun tietoturvasta.

Kuvan 4 esimerkkitoteutuksessa lähtötietojen keräämiseen liittyvä vastuu kuuluu kummankin C-ITS-keskusyksikköoperaattorin vastuulle (kansallinen C-ITS-operaattori ja kaupunki). Ne vastaavat käsittelemiensä tietojen luottamuksellisuudesta ja eheydestä. Kyseisiä toimijoita voi rinnastaa esimerkissä olennaista liikennepalvelua tuottaviksi toimijoiksi, jolloin niiden tietoturvallisuuden hallintaan sovelletaan NIS1 ja NIS2-direktiivien vaatimuksia. Esimerkissä C-ITS-palveluita tarjoavat C-ITS-keskusyksikköoperaattorit (ks. kuva 4, Appl. provider). Tällöin näiden tietoturvallisuuden hallintaa tulee ohjata standardin ISO 27001 mukaisen sertifioidun tietoturvallisuuden hallintajärjestelmän avulla. Samanaikaisesti kaikkia Kuvan 4 mukaisia C-ITS-yksikköoperaattoreita koskevat komission julkaiseman C-ITS-turvallisuuspolitiikan vaatimukset. Se vaatii operaattoreita arvioimaan jatkuvasti C-ITS-viestien muodostamiseen ja niiden käsittelyyn liittyviä turvallisuusriskejä sekä toteutukseen liittyvää yksityisyyden suojaa. Samat velvollisuudet koskevat myös hälytysviranomaista, joka toimii esimerkissä hälytysajoneuvoihin asennettujen C-ITS-ajoneuvoyksiköiden yksikköoperaattorina.

7 Tiedonvaihtopalvelimen vaatimukset ja toteutettavuus

7.1 Tiedonvaihtopalvelin

Tiedonvaihtopalvelimet ovat oleellinen osa Euroopan laajuista C-ITS-luottamusmalliin pohjautuvaa C-ITS-palvelutoteutusten arkkitehtuuria. Tiedonvaihtopalvelimet eivät kuulu C-ITS-luottamusalueeseen (C-ITS trust domain), vaan niillä on erityinen rooli toteuttaa pitkän kantaman tiedonsiirtoon perustuvissa C-ITS-ratkaisuissa kansallisten C-ITS-palvelutoteutusten sekä niiden sisältämien tienpitäjien ja palveluntarjoajien operoimien verkkojen välistä kommunikointia.

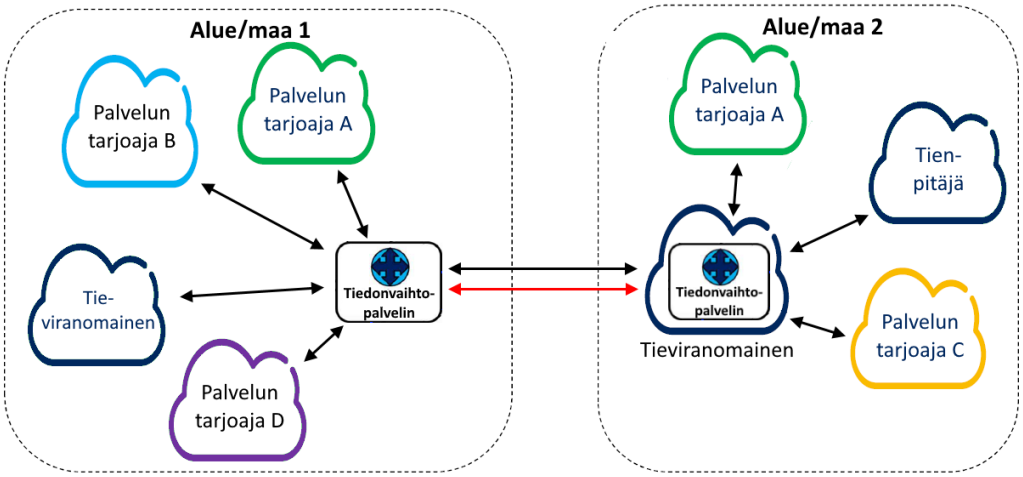
Tiedonvaihtopalvelimen toteutukselle tai operoinnille ei aseteta vaatimuksia C-ITS-turvallisuus- tai varmennepolitiikkadokumenteissa, eikä niiden tietoturvallisuuden hallinta tapahdu C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisesti.

Tiedonvaihtopalvelimien rooli ja liittyminen osaksi C-ITS-luottamusmalliin pohjautuvia verkkoja, tiedonvaihtopalvelimien välinen viestintä, tietoturvallisuus sekä niiden hallinnointimalli on kuvattu C-Roads-spesifikaatiossa C-ITS IP Based Interface Profile (C-ITS IP Based Interface Profile 2024). Tässä luvussa esitetyt tiedonvaihtopalvelimeen kohdistuvat määrittelyt ja vaatimukset perustuvat pääasiassa kyseiseen C-Roads-spesifikaatioon.

7.2 Tiedonvaihtopalvelimet osana C-ITS-toteutusten arkkitehtuuria

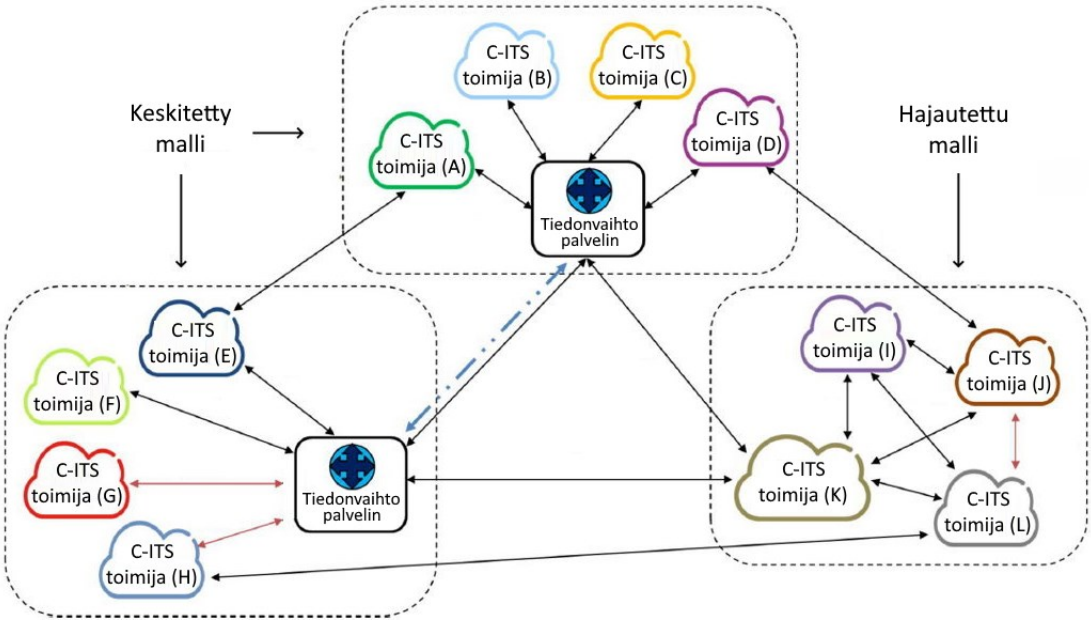
Tiedonvaihtopalvelimet yhdistävät toisiinsa kansallisia ja alueellisia C-ITS-palvelutoteutuksia sekä välittävät liikennettä niiden välillä. Alueellisesti tiedonvaihtopalvelimet kokoavat yhteen valtion ja kaupunkien (tienpitäjien) sekä ajoneuvovalmistajien ja yksityisten palveluntarjoajien operoimia C-ITS-palvelutoteutuksia. Kansallisesti ne mahdollistavat eri maissa syntyvien C-ITS-palvelutoteutusten välisen viestinnän.

Verkkoteknisesti tiedonvaihtopalvelimien viestintä tapahtuu IP-pohjaisissa verkkoympäristöissä, esimerkiksi avoimessa Internet-verkossa tai suljetuissa operaattoreiden IP-pohjaisissa laajaverkkoympäristöissä (Wide Area Network, WAN). Kyseisten verkkojen käyttöön, kuten verkkotekniseen toteutusarkkitehtuuriin (esim. avoin vai suljettu IP-verkko) C-Roads-spesifikaatiot eivät ota kantaa.



Kuva 5. Tiedonvaihtopalvelimien rooli kansallisten ja alueellisten C-ITS-palvelutoteutusten välisessä tiedonvaihdossa (mukaillen C-ITS IP Based Interface Profile 2023, 32).

C-Roads ei määrittele tarkasti alueellisissa toteutuksissa tiedonvaihtopalvelimien määrää tai niiden ja C-ITS-keskusyksiköiden välisiä suhteita. Kuvassa 6 on esitetty C-ITS-palvelutoteutusten ja tiedonvaihtopalvelimien välisiä mahdollisia verkkorakenteellisia toteutusmalleja.



Kuva 6. Tiedonvaihtopalvelimien ja alueellisten C-ITS-palvelutoteutusten (kuvassa C-ITS-toimija) välisiä erilaisia verkottumisrakenteita (mukaillen C-ITS IP Based Interface Profile 2023, 57).

Kuvan 6 esittämä C-ITS-toimijoiden[1] (C-ITS Actor) ja tiedonvaihtopalvelimien mukainen rakennekuva havainnollistaa C-Roadsin määrittelemän mallin joustavuutta alueellisten sekä kansallisten C-ITS-palvelutoteutusten välisen viestinnän toteutuksessa.

Kukin C-ITS-palvelutoteutus voi olla rakenteeltaan hyvin erilainen. Kuvan 6 hajautettu malli osoittaa, että useiden C-ITS-palvelutoteutusten välinen viestintä ei välttämättä tarvitse toimiakseen tiedonvaihtopalvelinta. Mallissa kaikki C-ITS-palvelutoteutukset, käytännössä niiden sisältämät C-ITS-keskusyksiköt, kommunikoivat keskenään niin, että tiedonvaihto kaikkien alueiden välillä mahdollistuu. Keskitetyssä mallissa rakenne on tähtimäinen. C-ITS-palvelutoteutusten C-ITS-keskusyksiköt eivät ole suorassa yhteydessä toisiinsa, vaan viestintä alueiden välillä tiedonvaihtopalvelimen kautta, vaikka tähtimäinen malli ei toisaalta kiellä erillisiä C-ITS-palvelutoteutusten välisiä suoria yhteyksiä (kuvassa A↔E).

[1] C-ITS-toimija (C-ITS Actor) on joukko C-ITS-järjestelmän toimintaan liittyviä organisaatioita tai henkilöitä, joilla on tiettyjä rooleja liittyen järjestelmään toimintaan ja sen käyttötapauksiin. Toimijat voivat olla esimerkiksi C-ITS-järjestelmän operointia toteuttavia tai C-ITS-tietoa käsitteleviä organisaatioita, kuten tienpitäjät tai C-ITS-yksikköoperaattorit. C-ITS-toimijat voivat olla esimerkiksi myös C-ITS-järjestelmän käyttäjiä. C-ITS-järjestelmien toimintaan liittyvät roolit, vastuut ja toimijat määritellään ISO:n standardissa 17427-1. (ISO 17427-1 2018)

7.3 Tiedonvaihtopalvelimien viestintä

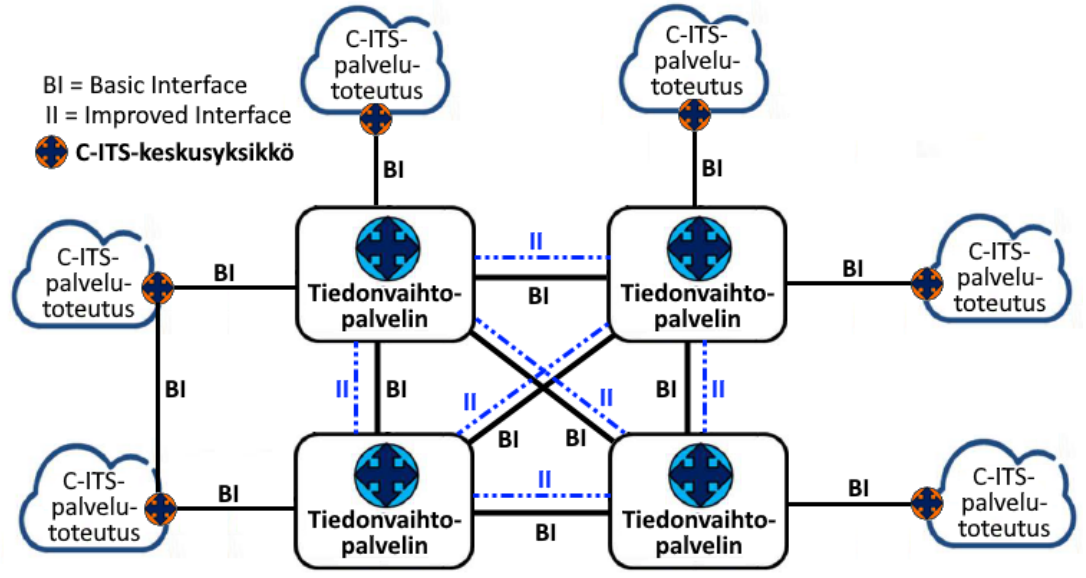
Tiedonvaihtopalvelimien viestinnällä tarkoitetaan palvelimien keskinäistä viestintää sekä tiedonvaihtopalvelimien ja alueellisten C-ITS-palvelutoteutusten C-ITS-keskusyksiköiden välistä viestintää, jota on kuvattu edellisen luvun kuvassa 6.

Tässä luvussa keskitytään kuvaamaan tiedonvaihtopalvelimien viestintään ja sen tietoturvallisuuteen liittyvät C-Roadsin asettamat vaatimukset. (C-ITS IP Based Interface Profile 2023, 32–51)

7.3.1 Tiedonsiirron protokollat

C-Roads määrittelee tiedonvaihtopalvelimien viestintään kolme protokollaa BI (Basic Interface), II (Improved Interface) sekä ISO:n standardoiman AMQP-protokollan (ISO/IEC 19464). BI- ja AMQP-protokollat on esitelty jo edellisessä C-ITS-yksiköitä käsittelevässä luvussa 6.

II-protokolla on tiedonvaihtopalvelimien välille toteutettu protokollalaajennus, joka tarjoaa BI-protokollan toiminnalle dynaamisen ohjauskerroksen tiedonvaihtopalvelimien taustalla sijaitsevien kansallisten ja alueellisten C-ITS-palveluiden tai tietolähteiden automaattiseksi löytämiseksi. Protokolla ehkäisee tarpeen kussakin C-ITS-alueessa sijaitsevien palveluiden manuaalisille määrittelyille. Näin se luo Euroopan laajuisesta useista eri hallinnollisista alueista koostuvasta C-ITS-palvelutoteutuksesta skaalautuvan ja dynaamisesti toimivan kokonaisuuden.



Kuva 7. Esimerkki pitkän kantaman tiedonsiirtoon perustuvien C-ITS-ratkaisujen taustalla toimivien taustajärjestelmien, C-ITS-keskusyksiköiden ja tiedonvaihtopalvelimien, muodostamasta verkostosta sekä järjestelmien välillä toimivista protokollista.

II-protokollan tekninen toimintakuvaus

Jotta tiedonvaihtopalvelinten verkosto olisi toimiva, tulee määrityksen mukaisesti jokaisen rekisteröityneen palvelimen muodostaa ohjauskanava toisiin aktiivisiin tiedonvaihtopalvelimiin käyttäen Improved Interface -protokollaa. Protokollan avulla mahdollistetaan tiedonvaihtopalvelimien väliset kyselyt. Kyselyjen avulla voidaan automaattisesti selvittää kuhunkin tiedonvaihtopalvelimeen liitetyt C-ITS-palvelut ja tietolähteet sekä tehdä näihin palveluihin liittyviä tilauksia eli

automaattisesti välittää C-ITS-palveluita Euroopan laajuisessa C-ITS-palvelutoteutuksen arkkitehtuurissa eri maiden alueellisten palvelutoteutusten välillä.

Tiedonvaihtopalvelimien väliset ohjauskanavat muodostetaan kaikkien yhteisesti käyttämällä tilausmenettelyllä (Subscription). Sen mukaisesti tiedonvaihtopalvelin pyytää toiselta palvelimelta tietoja varsinaisen tiedonvaihtokanavan muodostamista varten. Vastauksessa palautetaan kanavan vastapään tiedot (endpoint), jotka sisältävät osoite- sekä porttitiedot tiedonvaihtokanavan muodostamiseen.

Tiedonvaihtopalvelinten jatkuvaan toimintaan kuuluu, että ne ylläpitävät aktiivisesti tietoja toistensa tarjoamista C-ITS-palveluista sekä lähettävät muille osapuolille muutokset omista palveluistaan. Ne vastaanottavat C-ITS-palveluihin liittyviä tilauksia muilta tiedonvaihtopalvelimilta sekä välittävät automaattisesti muille tiedonvaihtopalvelimille omassa verkossaan olevien C-ITS-keskusyksiköiden tekemiä tilauksia. C-ITS-palveluilla tarkoitetaan kunkin tiedonvaihtopalvelimen tarjoamia tiettyihin maantieteellisiin alueisiin liittyviä C-ITS-palveluviestejä.

Ohjauskanavan muodostamiseen tarvittavat tiedonvaihtopalvelimien osoite- ja porttitiedot ovat saatavilla erillisestä DNS-rekisteristä[1], joka sisältää osoite- sekä porttitiedon ohjauskanavan osalta. DNS-rekistereitä säilytetään hallintoelimen ylläpitämässä vain C-ITS-palvelutoteutuksia varten toteutetussa DNS-palvelussa.

Tiedonvaihtopalvelimen operoijan vastuulla on pitää DNS-rekisterin tiedot ajan tasalla. Tiedonvaihtopalvelinten tulee myös päivittää vähintään 12 tunnin välein omat tietonsa muista aktiivisista palvelimista sekä niiden DNS-tietueista. Tiedonvaihtopalvelimien verkoston osana toimiva DNS-järjestelmän toiminta selostetaan myöhemmin luvussa 7.5.

Improved Interface -ohjauskanavan muodostamiseen hyödynnetään TLS-varmenteella suojattua HTTPS-protokollaa. Tietoturvan kannalta on myös määritetty, ettei yhteyttä tule sallia, jos yhteydenottajan tietoja ei löydy DNS-tietueista. TLS-varmenteisiin liittyvät vaatimukset on kuvattu tämän raportin luvussa 6.3.3.

Tiedonvaihtopalvelimen tulee kyetä vaihtoehtoisesti lukemaan ja ylläpitämään tietoja muiden palvelinten tarjoamista C-ITS-palveluista ja tarjota näitä tietoja siihen yhteydessä oleville C-ITS-keskusyksiköille tai pystyä ohjaamaan C-ITS-yksiköiden kyselyt toisiin tiedonvaihtopalvelimiin (redirect-policy). Tietoa tämän ominaisuuden (redirect) päällä olosta pidetään yllä tiedonvaihtopalvelinten metatiedoissa. Jos joku tiedonvaihtopalvelin määrittää omissa metatiedoissaan tämän ominaisuuden pakolliseksi, niin siihen yhteydessä olevien palvelinten tulee toteuttaa samaa toimintoa.

On myös hyvä huomioida, että II-rajapintatuki on valinnainen ominaisuus tiedonvaihtopalvelimelle (C-ITS IP Based Profile 2024, 33). Jos palvelin toteuttaa rajapintatuen, tulee sen täyttää C-Roadsin mukaiset vaatimukset. Ilman rajapintatukea tiedonvaihtopalvelimen rooli on rajallinen ja vain tietyt sen osat voidaan ottaa käyttöön tiedonvaihtopalvelimien välisillä kahdenvälisillä sopimuksilla.

[1] DNS (Domain Name System) on Internetissä tai muissa IP-verkoissa toimiva nimipalvelujärjestelmä. Se ylläpitää tietoja verkossa sijaitsevien tietokoneiden ja palveluiden IP-osoitteista ja osoitteisiin liittyvistä nimistä. Järjestelmän toiminta perustuu IETF:n (Internet Engineering Task Force) määrittelemiin dokumentteihin RFC 1034 ja 1035.

7.3.2 Tiedonsiirron salaus

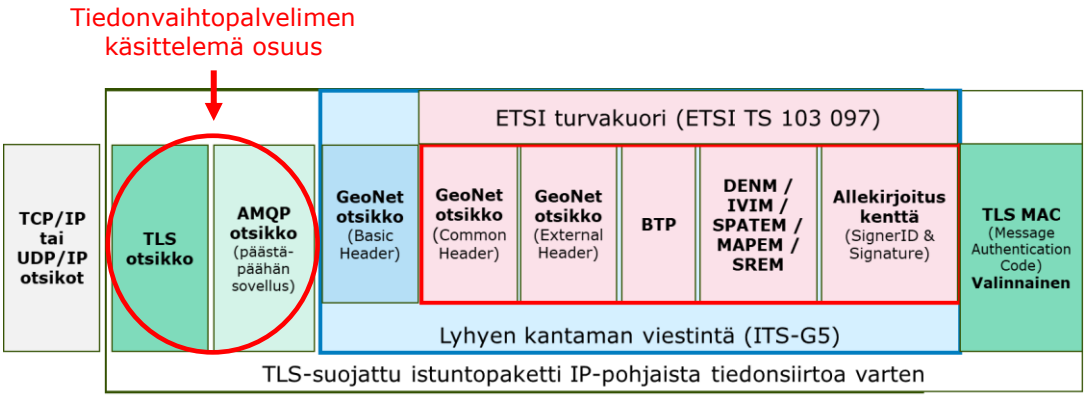
Luvussa 6.3.1 käsiteltiin C-ITS-viestien rakennetta eli viestinnässä käytettäviä eri protokollien muodostamia otsikkotasoja. Luvussa esitetyn mukaisesti IP-verkossa välitettävä C-ITS-viesti rakentuu käytännössä kahdesta osasta: (1) lyhyen kantaman tiedonsiirrossa käytettävästä osasta, joka sisältää varsinaisen C-ITS-viestin kannalta oleelliset tiedot, kuten C-ITS-viestityypin, viestin lähettäjään tai kohteeseen liittyvän paikkatiedon (GeoNetworking-protokolla) sekä varsinaisen C-ITS-viestin ja (2) IP-verkossa käytettävien protokollien otsikkokentistä.

Pitkän kantaman tiedonsiirron turvallisuus toteutetaan kahdella tasolla. Ensimmäinen taso tarkoittaa C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaista viestien allekirjoittamista PKI-menetelmän avulla (kuva 8, ETSI Security Envelope). Viestien allekirjoittamisella varmistetaan ETSI-turvakuoren sisällä olevien tietojen eheys ja lähettäjän luottamuksellisuuden. Lähettäjä allekirjoittaa turvakuoren sisällä olevat tiedot omalla salaisella PKI-avaimella (kuva 8, SignerID & Signature -kenttä) ja viestin vastaanottaja tarkastaa lähettäjän julkisen avaimen ja allekirjoituksen avulla, että tiedot eivät ole muuttuneet matkalla.

IP-verkossa C-ITS-keskusyksiköt ja tiedonvaihtopalvelimet lisäävät alkuperäiseen allekirjoitettuun ETSI-turvakuoren ulkopuolelle AMQP-protokollan mukaisen otsikkokentän (kuva 8 AMQP-otsikkokenttä). Tämä kenttä sisältää viestien reitittämiseksi ja suodattamiseksi tarvittavat tiedot, jotka on muodostettu ETSI-turvakuoren sisällä olevista tiedosta. Näistä tärkeimmät ovat tieto alkuperäisen C-ITS-viestin tyypistä sekä viestiin kohdistuva maantieteellinen sijainti ns. QuadTree-tietorakenteen[1] avulla koodattuna. Näiden tietojen avulla tiedonvaihtopalvelimen ei tarvitse käsitellä ETSI-turvakuoren sisällä olevia tietoja, jolloin se voi tehdä viestien suodatusta ja reititystä pelkästään AMQP-protokollan muodostaman otsikkokentän avulla. Tiedonvaihtopalvelin ei myöskään tarkasta viestin allekirjoitusta.

IP-verkon viestinnän toinen turvallisuustaso toteutetaan taustapalvelinten välisillä istunnoilla. ETSI-turvakuori ja AMQP-otsikkokenttä muodostavat lopullisen viestin, joka salataan kahden taustajärjestelmän väliselle yhteydelle (istunnolle) TLS-salausprotokollan avulla ja välitetään lopuksi järjestelmien välillä TCP/IP-protokollien avulla. Vastaanottava palvelin purkaa salauksen ja pystyy toteuttamaan viestien reititystä ja suodatusta AMQP-protokollan metatietokenttien avulla.

[1] Quadtree on yleisesti paikkatietojärjestelmissä käytetty tietorakenne, jossa jokaisella sen sisäisellä solmulla on neljä lasta. Sitä käytetään jakamaan kaksiulotteinen tila (tietokoneen ruutu tai kartta) toistuvasti neljään osaan tai alueeseen. Tietorakenne nimettiin Quadtreeksi Raphael Finkelin ja J.L. Bentleyn toimesta vuonna 1974.



Kuva 8. Kuvassa on esitetty pitkän kantaman tiedonsiirrossa tiedonvaihtopalvelimen käyttämä osuus viestinnän paketeista (mukaillen C-ITS Security & Governance 2023, 12).

7.3.3 Välityskapasiteetin skaalaaminen

C-Roads määrittelee viestivirran käsittelyn liittyvän ”sharding”-ominaisuuden C-Roads-spesifikaation C-ITS IP Based Interface Profile liitteessä G.

Sharding-ominaisuus mahdollistaa suurista välitettävistä viestivirroista johtuvan tarpeen toteuttaa viestien käsittelyä hajautetusti useissa viestien välitysyksiköissä. Ominaisuuden avulla C-ITS-viestit voidaan optimaalisesti hajauttaa sovitulle määrälle välitysyksiköitä ja järjestää oikeaan järjestykseen hajautetun käsittelyn jälkeen. Viestien välityskapasiteetin parantamista useiden välitysyksiköiden avulla kutsuteen horisontaaliseksi skaalaamiseksi. Toinen vaihtoehto välityskyvyn skaalaamiseksi olisi välityskyvyn parantaminen laskentatehon lisäämisellä yhteen tiedonvaihtopalvelimeen (vertikaalinen skaalaaminen).

C-ITS-järjestelmän osana toimivat tiedonvaihtopalvelimet, jotka käyttävät useampia välitysyksiköitä C-ITS-viestien käsittelyyn, ilmoittavat sharding-ominaisuuden käytöstä II-protokollan avulla muille yksiköille (shardCount > 1). Tämän ilmoituksen perusteella lähettävät C-ITS-yksiköt osaavat jakaa lähetettävän tietovirran optimaalisesti vastaanottavan tiedonvaihtopalvelimen laskentayksiköiden määrän mukaisesti. Lähetettävät C-ITS-paketit jaetaan ja merkitään laskentayksiköiden määrän mukaisesti ja järjestysnumeroidaan. Näiden tietojen perusteella paketit jakaantuvat vastaanottajan päässä eri palvelimille (kuormanjako) ja ne voidaan järjestää hajautetun käsittelyn jälkeen takaisin alkuperäiseen järjestykseen

7.3.4 Istuntokohtaiset luottamusalueet

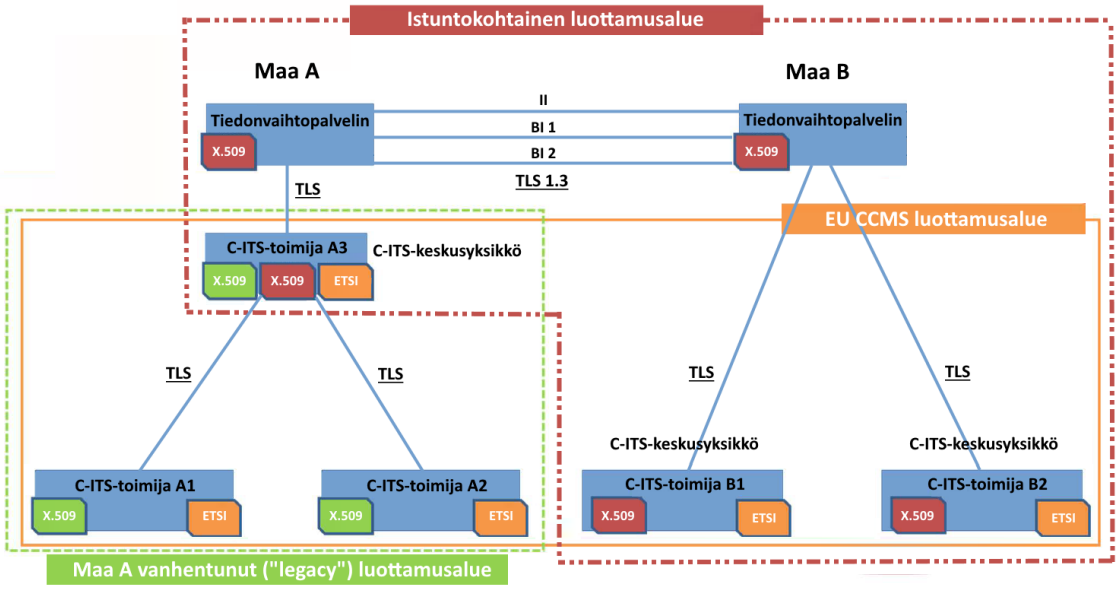
Kuvassa 9 on esitetty C-ITS-palvelutoteutusten arkkitehtuureissa käytettävien taustajärjestelmien välisiin yhteyksiin liittyvät istuntokohtaiset luottamusalueet (trust domain). Kuvassa luottamusalueet jaetaan kolmeen erilaiseen alueeseen.

(1) Punainen viiva, istuntokohtainen luottamusalue, joka toimii C-Roadsin määrittelemällä istuntojen tietoturvan toteuttavalla C-Roadsin mukaisalla TLS1.3-suojausprotokollalla sekä X.509-varmenteilla.

(2) Oranssi viiva, C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen luottamusalue, jossa C-ITS-keskusyksiköt allekirjoittavat tai tarkastavat viestit

allekirjoituksen perusteella (istunnot myös salataan alueella TLS-suojausprotokollalla, mutta kaikki yksiköt eivät tue C-Roadsin mukaista tapaa, vihreä rajaus).

(3) Vihreä katkoviiva, maakohtainen C-ITS-alue, joka ei tue samaa C-Roadsin määrittelemää TLS-standardi- tai X.509-varmenneversiota (”legacy trust domain”), jolloin se ei voi liittyä C-Roadsin määrittelemään istuntokohtaiseen luottamusalueeseen, mutta toisaalta toteuttaa C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaista ETSI-turvakuorimenettelyä.



Kuva 9. C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) ja pitkän kantaman tiedonsiirtoratkaisuissa käytettävien taustajärjestelmien välisen viestinnän luottamusalueet (C-ITS IP Based Interface Profile 2023, 63).

7.4 Tiedonvaihtopalvelimien operointi

C-Roads ei määrittele tiedonvaihtopalvelimen operoinnille suoraan vaatimuksia, kuten Euroopan komission turvallisuus- ja varmennepolitiikka määrittelee C-ITS-yksiköiden operoinnille (ks. luku 4).

Tiedonvaihtopalvelimien ja C-ITS-keskusyksiköiden operointiin liittyviä erilaisia vaatimuksia voidaan perusteella niiden erilaisella roolilla C-ITS-järjestelmässä. C-ITS-keskusyksiköt muodostavat C-ITS-viestejä ja allekirjoittavat niitä. Tämä toiminta asettaa C-ITS-keskusyksiköiden operaattorit vastuuseen muodostettavien C-ITS-viestien taustalla olevien lähtötietojen luotettavuudesta sekä viesteihin liittyvistä tietoturvauhista. Samalla keskusyksiköiden operaattorit vastaavat allekirjoituksiin käytettävien PKI-avainten hallinnasta. Näiden toimien tietoturvalliseen hallintaan liittyen C-ITS-turvallisuuspolitiikka asettaa vaatimuksen C-ITS-yksiköiden operoijille mm. standardin ISO 27001 mukaisesta sertifioidusta tietoturvallisuuden hallintajärjestelmästä. Tiedonvaihtopalvelimet eivät muodosta tai allekirjoita C-ITS-viestejä eivätkä hallinnoi niihin liittyviä PKI-avaimia. Näiden erojen vuoksi tiedonvaihtopalvelimia operoivilta tahoilta ei vaadita vastaavaa sertifioitua tietoturvallisuuden hallintajärjestelmää.

Vaikka tiedonvaihtopalvelimiin ei kohdistu yllä esitetyn mukaisesti samoja vaatimuksia kuin C-ITS-keskusyksiköille, ne ovat tärkeä osa tulevaa C-ITS-järjestelmää ja niiden yhteiseurooppalaista toimintaa. Euroopan kyberturvallisuusdirektiivi

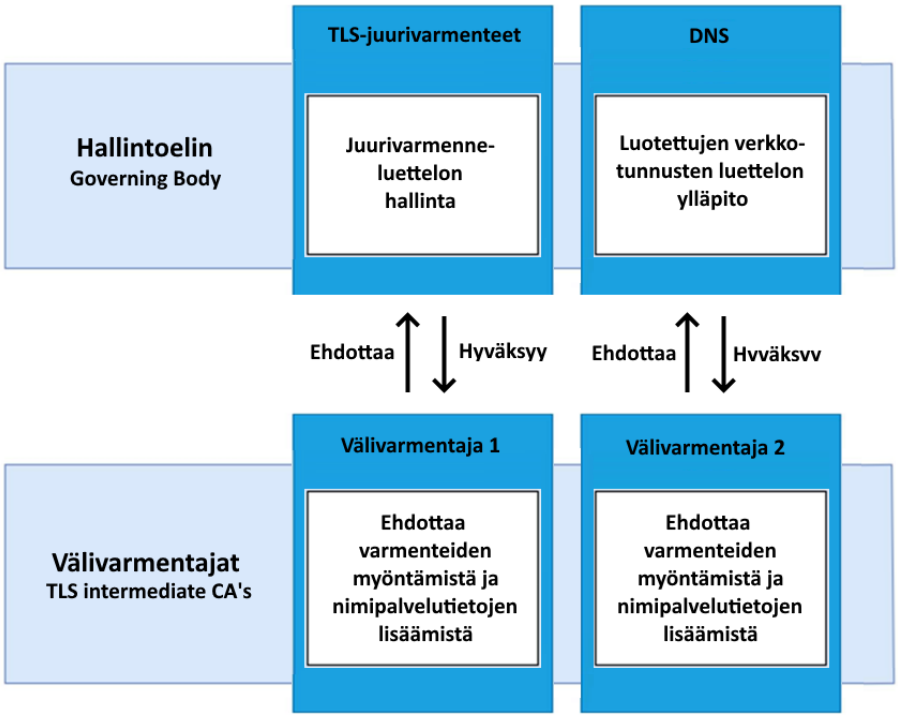
luokittelee liikennealan kriittiseksi toimialaksi, jonka parissa toimivia toimijoita (esim. tienpitäjät, kunnat ja suuret yksityiset organisaatiot) koskevat NIS2-kyberturvallisuusdirektiivin vaatimukset, johon perustuen tiedonvaihtopalvelimen ja sen operoinnin voidaan nähdä olevan NIS2-direktiivin vaatimusten alainen (EU 2022/2555 2022 sekä EU 2010/20/EU 2010)[1].

7.5 Tiedonvaihtopalvelimien verkoston hallinnointimalli

Luvussa 7.2 (Tiedonvaihtopalvelimien viestintä) käsiteltiin tiedonvaihtopalvelimen viestintään liittyviä tietoturvallisuuden vaatimuksia. Luvun mukaisesti tiedonvaihtopalvelimien välisten yhteyksien suojaamiseksi käytetään Internet-verkon toiminnasta tuttua TLS-suojausprotokollaa ja X.509-varmenteita.

Yllä kuvattujen (luvut 7.3 ja 7.4) tietoturvallisuusratkaisujen lisäksi tiedonvaihtopalvelimien ja pitkän kantaman tiedonsiirtoon perustuvien C-ITS-palvelutoteutusten taustajärjestelmien välisessä viestinnässä käytetään hyväksi Internet-verkosta tuttua DNS-nimipalvelujärjestelmää.

C-Roadsin määritysten mukainen istuntopohjainen tietoturva ja DNS-nimipalvelujärjestelmän käyttö eivät kuitenkaan käytä Internet-verkossa julkisesti käytössä olevia varmennetoimijoita tai DNS-nimipalveluita. C-Roads määrittelee näiden palveluiden käytölle C-ITS-järjestelmien taustajärjestelmien toiminnassa oman hallinnollisen suljetun mallin. Hallinnollisen mallin keskeiset elimet ja toiminnot on esitetty kuvassa 10.



Kuva 10. Kuvassa on esitetty C-Roadsin hallintomallin toimijat ja niiden väliset suhteet (C-ITS IP Based Interface Profile 2023, 63).

[1] NIS2-direktiivin liite 1 määrittelee erittäin kriittisten toimialojen joukkoon liikenteenhallinnasta vastaavat viranomaiset sekä ITS-direktiivin 2010/40/EU 4 artiklan alakohdassa 1 määriteltyjen älykkäiden liikennejärjestelmien ylläpitäjät. ITS-direktiivi määrittelee älykkäiksi liikennejärjestelmiksi mm. järjestelmät, joissa sovelletaan tieto- ja viestintäteknologiaa tieliikenteen alalla.

Hallinnollinen malli perustuu erikseen perustettavan hallintoelimen toimintaan (”Governing Body”). Hallintoelimen vastuulla on TLS-juurivarmennepalvelun toiminta ja hallinta sekä tiedonvaihtopalvelimen viestintään käytettävän luotettavien DNS-palvelimen hallinnointi (DNS-tietueiden lisääminen ja poistaminen).

Hallintoelin on hallintomallin ylin toimija ja sen vastuulla on seuraavat toimenpiteet:

- TLS-juurivarmenteiden hallinnointi (Root CA)
- välivarmentajien (”TLS intermediate CA”) hyväksyntä
- luotettujen verkkotunnusten DNS-tietueiden hallinta
- tiedonvaihtoyksiköiden hyväksyntä luotettujen verkkotunnusten listaan välivarmentajien suositusten perusteella
- luotettujen verkkotunnusten luettelon ylläpito
- peruutettujen varmenteiden julkaisu.

Välivarmentajien vastuulla on vastaavasti:

- hyväksyä C-ITS-toimijat ja ehdottaa TLS-varmenteiden myöntämistä hallintoelimelle
- ehdottaa tiedonvaihtopalvelinta tai C-ITS-keskusyksikköä lisättäväksi hallintoelimen ylläpitämään luotettujen verkkotunnusten DNS-tietueisiin.

C-Roads ei määrittele hallintomallin toimijoiden tarkkaa nimeämistapaa tai mallia, jonka mukaan hallintoelin muodostetaan. Karkeasti voidaan olettaa, että koko Euroopan tasoisen hallintoelimen muodostaminen tulee luultavasti olemaan komission, varmennepolitiikkaviranomaisen, vastuulla. Välivarmentajakerroksen toimijat ovat kansallisia tai alueellisia vastuullisia toimijoita, jotka ehdottavat omalle alueelleen syntyviä C-ITS-keskusyksiköitä ja tiedonvaihtopalvelimia lisättäväksi hallintomallin mukaisen toiminnan osaksi.

7.6 Tiedonvaihtopalvelimien verkostovaikutukset

Tässä luvussa käsitellään tiedonvaihtopalvelimien käyttöönoton tuottamia hyötyjä C-ITS-palveluiden käyttöönotossa. Hyötyjä tarkastellaan tiedonvaihtopalvelimien tuottamien verkostovaikutusten näkökulmasta. Tiedonvaihtopalvelimien käyttöönoton tuottamia verkostovaikutuksia arvioidaan kolmesta eri näkökulmasta.

- Loppukäyttäjien saatavuuden paraneminen
- Eri palvelutoteutusten teknologiariippumattomuuden edistäminen
- C-ITS-palveluiden toteuttamisen helppous

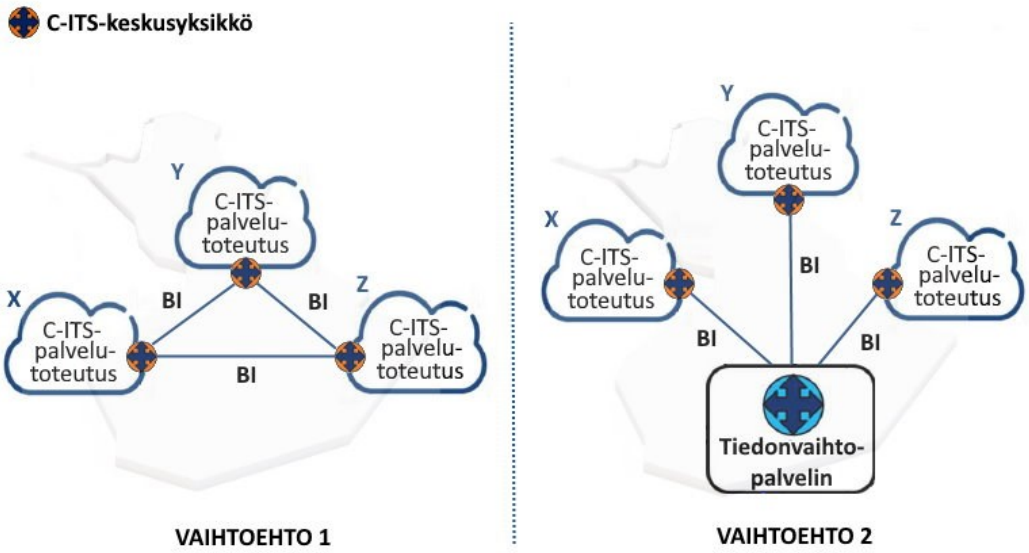
Kaikilla näillä näkökulmilla on C-ITS-palvelutoteutusten käyttöönottoa helpottava ja samalla C-ITS-palveluiden ja loppukäyttäjien saatavuutta edistävä vaikutus. Näistä syistä niiden voidaan olettaa tehokkaasti edistävän C-ITS-palveluiden leviämistä uusien palvelualueiden ja -toteutusten muodossa Euroopan laajuisesti.

Verkostovaikutuksia on aikaisemmin selvitetty vain lyhyen kantaman tiedonsiirtoon perustuvassa tutkimuksessa, jossa pyrittiin selvittämään C-ITS-ajoneuvoyksiköiden käytön lisääntymisen vaikutuksia C-ITS-palveluiden saatavuuteen. Käytännössä työssä pyrittiin selvittämään ehdollisen todennäköisyyden analyysin avulla, kuinka todennäköisesti C-ITS-ajoneuvoyksiköllä varustettu ajoneuvo voi vastaanottaa ajoneuvojen väliseen tiedonsiirtoon perustuvan C-ITS-viestin ajoneuvoyksiköiden penetraatioasteen kasvaessa. (Öörni 2024)

Tässä luvussa tiedonvaihtopalvelimien verkostovaikutusten tarkastelu tehdään erikseen kahdessa eri toimintaympäristössä: (1) tiedonvaihtopalvelimet osana kansallista C-ITS-palvelutoteutusten arkkitehtuuria sekä (2) tiedonvaihtopalvelimet osana yhteiseurooppalaista C-ITS-palvelutoteutusten arkkitehtuuria.

7.6.1 Tiedonvaihtopalvelin osana kansallista C-ITS-palvelutoteutusten arkkitehtuuria

Tiedonvaihtopalvelimen mahdollinen rooli kansallisissa C-ITS-palvelutoteutuksissa on toimia alueellisten C-ITS-palvelutoteutusten välisenä yhdysliikennepisteenä. Aikaisemmin luvussa 7.2 on kuvattu erilaisia alueellisten C-ITS-palvelutoteutusten välisiä verkottumisrakenteita (ks. kuva 6, s. 81). Kuvasta 6 voidaan nähdä, että C-Roads ei tarkkaan määrittele alueellisten C-ITS-palvelutoteutusten välistä verkottumismallia. Kuvassa esitettyjen verkottumismallien perusteella voidaan todeta, että C-ITS-palvelutoteutusten C-ITS-keskusyksiköt voivat kommunikoida suoraan keskenään (”hajautettu malli”) tai ne voivat kommunikoida keskenään yhden tiedonvaihtopalvelimen välityksellä (”keskitetty malli”). Kumpikin tapa mahdollistaa saman asian eli C-ITS-viestejä voidaan siirtää C-ITS-palvelutoteutusten välillä. Näitä kahta eri vaihtoehtoa on vielä erikseen havainnollistettu alla kuvassa 11.



Kuva 11. Tiedonvaihtopalvelimen roolin havainnollistaminen kansallisessa C-ITS-palveluiden arkkitehtuuriesimerkissä.

Alla on arvioitu tiedonvaihtopalvelimen tuottamia verkostovaikutuksia aikaisemmin esitettyjen tarkastelunäkökulmien avulla.

<u>Loppukäyttäjien saatavuuden paraneminen</u>

Kuvan 11 mukaiset vaihtoehdot osoittavat, että kumpikin verkottumisarkkitehtuuri mahdollistaa C-ITS-viestien välittämisen eri palvelualueiden välillä. Käytännössä tämä tarkoittaa, että kullakin palvelualueella (X, Y, Z) toteutettuja C-ITS-palveluita voidaan tarjota kaikkien palvelualueiden loppukäyttäjille. Tämän perusteella voidaan todeta, että tämän kaltaisessa kansallisessa toteutuksessa tiedonvaihtopalvelin ei varsinaisesti edistä loppukäyttäjien saavutettavuuteen liittyviä verkostovaikutuksia. Samat vaikutukset saadaan myös aikaiseksi verkottamalla C-ITS-palvelualueiden C-ITS-keskusyksiköt toisiinsa.

Teknologiariippumattomuuden edistäminen

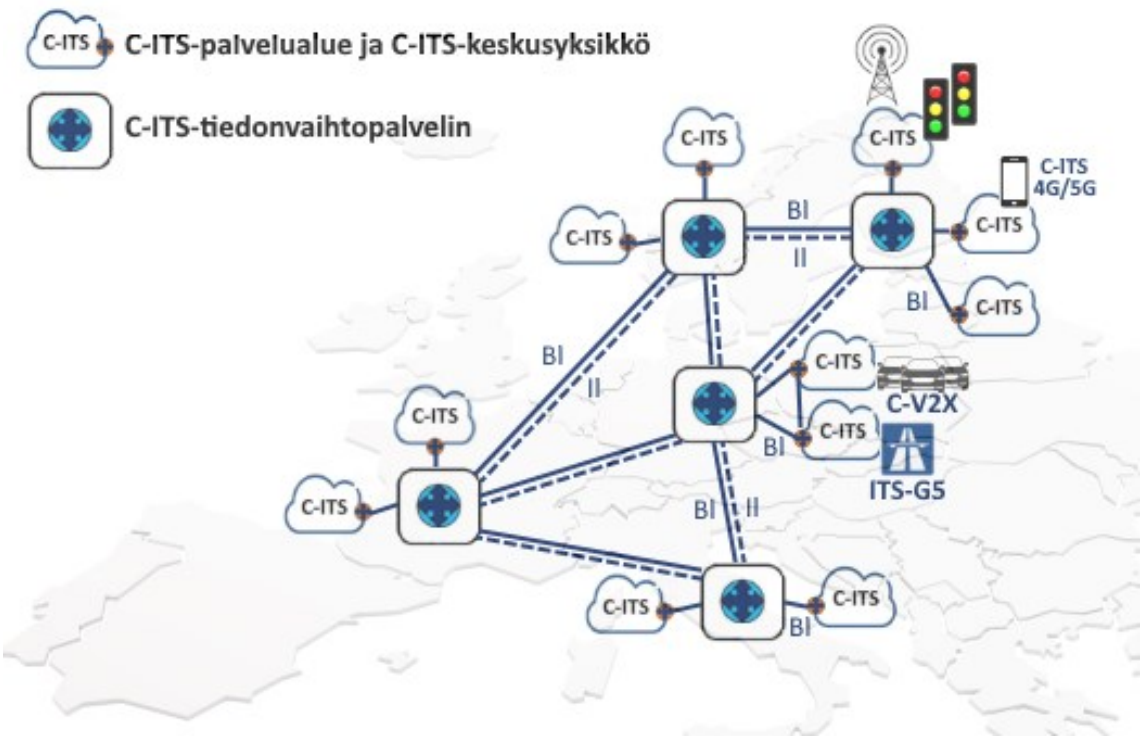
Edellisessä kohdassa esitetty lopputulos koskee myös teknologiariippumattomuuden edistämistä. Kummassakin kuvan 11 vaihtoehdossa kukin C-ITS-palvelutoteutus voi olla eri tiedonsiirtotavoilla toteutettu (lyhyt tai pitkä kantama) ja viestejä voidaan välittää palvelutoteutusten välisillä suorilla C-ITS-keskusyksiköiden välisillä linkeillä tai keskitetysti tiedonvaihtopalvelimen kautta. Kumpikin ratkaisu siis edistää C-ITS-palvelutoteutusten teknologiariippumattomuutta yhtä paljon.

C-ITS-palveluiden helpompi toteuttaminen

C-ITS-palveluiden toteuttamisen helppouteen liittyen tiedonvaihtopalvelimella voidaan olettaa olevan positiivinen vaikutus. Tämä näkökulma on helppo havaita myös kuvan 11 avulla. Vaihtoehdossa 2 yksittäisen C-ITS-palvelutoteutuksen on mahdollista saavuttaa kaikki muut palvelutoteutukset vain yhden keskusyksikön ja tiedonvaihtopalvelimen välisen linkin avulla. Tämän piirteen vaikutus kasvaa sitä suuremmaksi, mitä enemmän erillisiä C-ITS-palvelutoteutuksia kansalliseen C-ITS-arkkitehtuuriin muodostuu.

7.6.2 Tiedonvaihtopalvelin osana eurooppalaista C-ITS-palvelutoteutusten arkkitehtuuria

Tässä alaluvussa tiedonvaihtopalvelimen roolia tarkastellaan osana yhteiseurooppalaista C-ITS-arkkitehtuuria. Yhteiseurooppalainen C-ITS-arkkitehtuuriesimerkki on esitetty alla kuvassa 12.



Kuva 12. Tiedonvaihtopalvelimet osana yhteiseurooppalaisessa C-ITS-arkkitehtuuria.

Kuvassa 12 on esitetty yhteiseurooppalaiseen C-ITS-arkkitehtuuriin toteutettuja C-ITS-palvelutoteutuksia ja toteutuksia yhdistäviä tiedonvaihtopalvelimia. Kuvassa on esitetty myös esimerkkejä eri teknologioilla toteutetuista C-ITS-

palvelutoteutuksista. Suomen kohdalla on esitetty matkaviestinverkkoteknologioihin perustuva pitkän kantaman tiedonsiirron C-ITS-toteutus, johon on liitetty kiinni kansallisesti liikennevaloja ja palveluita hyödynnetään mobiilisovellusten avulla. Keski-Euroopassa ajoneuvoilla merkitty C-ITS-palvelutoteutus kuvaa yhden autovalmistajan ajoneuvojoukkoa, jotka on varustettu C-V2X-teknologiaa tukevilla C-ITS-ajoneuvoyksiköillä. Moottoritiesymbolilla merkitty keskieurooppalainen C-ITS-palvelutoteutus kuvaa paikallisen tienpitäjän ITS-G5-teknologialla toteuttamaa maan kattavan moottoritieverkoston laajuista palvelutoteutusta.

Kuvan 12 mukaisessa esimerkkiarkkitehtuurissa C-ITS-toteutus on laajentunut yhtenäiseksi eurooppalaiseksi C-ITS-arkkitehtuuriksi. Siinä C-Roadsin ja C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten mukaisesti toimivista tiedonvaihtopalvelimista ja C-ITS-keskusyksiköistä muodostettu verkosto mahdollistaa C-ITS-viestien välityksen palvelualueiden välillä. Teoriassa eri C-ITS-palvelualueiden väliset yhteydet voitaisiin tässäkin esimerkissä toteuttaa kuvan 11 tavoin toteuttamalla yhteydet kaikkien C-ITS-keskusyksiköiden välille. Käytännön tasolla tämä ei kuitenkaan enää ole näin laajassa C-ITS-arkkitehtuurissa järkevää. Tiedonvaihtopalvelimien mahdollistama II-protokollan (Improved Interface) hyödyntäminen on myös oleellinen osa yhteiseurooppalaisen C-ITS-arkkitehtuurin toimintaa. Se mahdollistaa tiedonvaihtopalvelimien välisen C-ITS-palveluiden mainostamisen, jolloin tiedonvaihtopalvelimet lähettävät automaattisesti toisilleen tiedon eri C-ITS-palvelualueille syntyneistä uusista C-ITS-palveluista. Tämä helpottaa merkittävästi C-ITS-toteutuksen ylläpitoa ja tehokasta toimintaa.

Alla on arvioitu tiedonvaihtopalvelimien tuottamia verkostovaikutuksia kuvan 12 mukaisen yhteiseurooppalaisen C-ITS-arkkitehtuurin osana.

Loppukäyttäjien saatavuuden paraneminen

Loppukäyttäjien saatavuuden paranemista tarkastellaan kuvan 12 mukaisten esimerkkien avulla.

Esimerkki 1

Kuvassa autovalmistajan C-ITS-palvelualueeseen liitetyt C-V2X-teknologiaa tukevat ajoneuvot voivat hyödyntää Suomeen toteutettuja pitkän kantaman tiedonsiirtoon perustuvia sekä paikallisen tienpitäjän ITS-G5-pohjaisia C-ITS-palveluita. Suomessa liikkuessaan esimerkiksi liikennevaloilta välitetyt C-ITS-viestit voidaan välittää palvelualueen C-ITS-keskusyksikön ja suomalaisen tiedonvaihtopalvelimien kautta autovalmistajan C-ITS-keskusyksikölle, joka mahdollistaa liikennevaloihin liittyvien C-ITS-palveluiden tarjoamisen ajoneuvoille. Saman voi toteuttaa myös paikallinen tienpitäjä. Viestit voidaan välittää ITS-G5-teknologiaa tukevien tienvarsiyksiköiden kautta tienpitäjän C-ITS-keskusyksikölle, josta ne on mahdollistaa välittää tiedonvaihtopalvelimen ja autovalmistajan C-ITS-keskusyksikön kautta C-V2X-teknologiaa tukeville ajoneuvoyksiköille. Kuvan 12 esimerkissä näiden kahden C-ITS-palvelualueen väliseen viestintään on myös toteutettu C-ITS-keskusyksiköiden välinen suora yhteys.

Esimerkki 2

Suomalaiset mobiilisovellusta käyttävät C-ITS-loppukäyttäjät voivat saada keskieurooppalaisen moottoritien C-ITS-palvelualueelle liikkuessaan esimerkiksi tietyömaiden varoitusviestejä. Varoitusviestit voidaan välittää moottoritielle

asennettujen C-ITS-tienvarsiyksiköiden (RSU) välityksellä paikallisen tienpitäjän ylläpitämälle C-ITS-keskusyksikölle, josta ne välittyvät tiedonvaihtopalvelimien kautta suomalaisen C-ITS-palveluntarjoajan keskusyksikölle ja sieltä mobiilipäätelaitteen C-ITS-sovellukselle.

Esimerkkien mukaisesti voidaan todeta, että tiedonvaihtopalvelimella on merkittävä rooli eurooppalaisen C-ITS-järjestelmän loppukäyttäjien saatavuuden edistäjänä.

Teknologiariippumattomuuden edistäminen

Edellisen kohdan esimerkkeihin viitaten tiedonvaihtopalvelimet mahdollistavat useissa tapauksissa alueellisten C-ITS-palveluiden hyödyntämisen, vaikka loppukäyttäjät käyttävät eri teknologioita kuin C-ITS-palvelualue, jossa ajoneuvot liikkuvat.

Kaikkia mahdollisia C-ITS-tiedonsiirtotapoja tiedonvaihtopalvelimet eivät kuitenkaan ratkaise. Eri teknologioilla varustettujen ajoneuvojen välinen suora viestintä ei esimerkissä ole mahdollista, joskin monissa tapauksissa se voidaan toteuttaa C-ITS-keskusyksiköiden ja tiedonvaihtopalvelimien kautta. Tässä tarkastelussa ei kuitenkaan oteta ajoneuvojen väliseen viestintään liittyen kantaa voivatko kaikki ajoneuvojen väliset V2V-palvelut (Vehicle-to-Vehicle) toimia C-ITS-taustajärjestelmien kautta välitettynä riittävän nopeasti. Yhtenä esimerkkinä on ajoneuvojen välillä välitetty tieto ajoneuvon toteuttamasta hätäjarrutuksesta (Emergency Brake Light, EBL).

ITS-G5-tekniikalla varustetut ajoneuvot olisivat esimerkissä hankalinta saavuttaa (näitä ei ole esitetty kuvassa). Ne voitaisiin saavuttaa vain C-ITS-palvelualueilla, joissa on käytössä samaa teknologiaa tukevat C-ITS-tienvarsiyksiköt.

Lopputuloksena voidaan kuitenkin todeta, että vaikka C-ITS-keskusyksiköiden välisillä yhteyksillä voitaisiin toteuttaa osittaisia C-ITS-palvelualueiden yhdistämisiä, niin tiedonvaihtopalvelimet edistävät merkittävästi teknologiariippumattomuutta yhteiseurooppalaisessa C-ITS-arkkitehtuurissa.

C-ITS-palveluiden helpompi toteuttaminen

C-ITS-palvelualueen sisäisten palveluiden toteutukseen tiedonvaihtopalvelimista ei ole hyötyä. Kuitenkin palvelualueen C-ITS-keskusyksikön liittäminen lähimpään tiedonvaihtopalvelimeen mahdollistaa oman palvelualueen palveluiden levittäminen Euroopan laajuisesti lähes kaikille palveluiden käyttäjille. Samalla tiedonvaihtopalvelimet helpottavat merkittävästi C-ITS-palvelualueen liittymistä osaksi yhteiseurooppalaista C-ITS-arkkitehtuuria.

Yhteenvetona voidaan todeta, että tiedonvaihtopalvelimet edistävät merkittävästi C-ITS-palveluiden helpompaa toteutusta.

7.6.3 Yhteenveto

Tiedonvaihtopalvelimien verkostovaikutuksia tutkittiin edellisissä alaluvuissa kahdessa eri ympäristössä: tiedonvaihtopalvelimet osana kansallista sekä yhteiseurooppalaista C-ITS-arkkitehtuuria.

Luvussa 7.6.1 esitetyn tarkastelun perusteella tiedonvaihtopalvelimet tuottavat joitakin positiivisia verkostovaikutuksia kansallisessa esimerkkiarkkitehtuurissa

(kuva 11, s. 89). Tiedonvaihtopalvelimet edistävät erityisesti kansallisten C-ITS-palveluiden liitettävyyttä toisiinsa, jolloin ne helpottavat palvelualueiden välisen viestinnän toteutusta. Tämä positiivinen vaikutus korostuu, kun C-ITS-palvelualueiden määrä kansallisessa toteutuksessa kasvaa.

Luvussa 7.6.2 käsiteltiin tiedonvaihtopalvelimien roolia osana yhtenäistä C-Roadsin ja C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimusten mukaista C-ITS-arkkitehtuuria. Luvussa tunnistettiin, että tiedonvaihtopalvelimilla on merkittävä rooli C-ITS-palveluiden ja niiden loppukäyttäjien saatavuuden edistämisessä. Samalla ne edistävät C-ITS-palvelualueiden teknologiariippumattomuutta sekä C-ITS-palveluiden toteuttamisen helppoutta.

7.7 Tiedonvaihtopalvelimien hankintamallit

Tiedonvaihtopalvelimien hankintaan liittyen tunnistetaan tyypillisiä IT-järjestelmien hankintaan liittyviä malleja. Nämä mallit eivät ole standardeissa tai C-Roads-spesifikaatioissa kuvattuja, eikä niitä kohtaan ole olemassa julkisia hankintoja koskevasta lainsäädännöstä eroavia vaatimuksia.

Tässä luvussa esitellään neljä erilaista lähestymistapaa tiedonvaihtopalvelimen hankintaan liittyen: avoimen lähdekoodin yhteisötoiminta, räätälöity toteutus, räätälöity toteutus avoimen lähdekoodin pohjalta ja tuotehankinta. Nämä kuvaukset eivät ole vielä suosituksia suomalaisesta mallista, vaan tuovat esille mallien toimintaa ja niihin liittyviä yleisiä näkökulmia.

7.7.1 Avoimen lähdekoodin yhteisötoiminta

Tässä alaluvussa käsitellään avoimen lähdekoodin yhteisötoimintaan perustuvaa ohjelmistoratkaisujen kehitystä. Alaluvun sisältö perustuu suurelta osin COSS ry:n (The Finnish Centre for Open Systems and Solutions) kanssa pidettyyn asiantuntijahaastatteluun (COSS ry haastattelu 2024). COSS ry on Suomen avoimien tietojärjestelmien keskus, joka edistää avoimen lähdekoodin ja avoimien teknologioiden hyödyntämistä yksityisellä ja julkisella sektorilla. Toinen keskeinen luvussa käytetty lähde on Euroopan komission vuonna 2021 toteuttamaan tutkimukseen avoimen lähdekoodin vaikutuksista Euroopan teknologiseen omavaraisuuteen, kilpailukykyyn ja innovaatiokyvykkyyksiin (Blind et al. 2021) sekä selvitystyöryhmän omaan asiantuntemukseen.

EU ja avoin lähdekoodi

Euroopan unionin Open Source -strategia (EU Open Source Strategy 2020–2023) rohkaisee hyödyntämään avoimen lähdekoodin ratkaisuja. Visiona on rohkaista ohjelmistoratkaisujen, tiedon ja asiantuntemuksen jakamiseen ja uudelleenkäyttöön paremman tuoton saavuttamiseksi ohjelmistokehityksessä. Vaikka strategia päättyi muodollisesti vuoteen 2023, käytännön toimet avoimen lähdekoodin ohjelmistojen tukemiseksi ovat jatkuneet, ja tavoitteena on yhä vahvistaa unionin digitaalista itsenäisyyttä, edistää avoimuutta sekä lisätä teknologian kehitystä ja yhteistyötä.

EU on myös linjannut avoimen lähdekoodin hyödyntämisen yhdeksi tavaksi edesauttaa EU-alueen digitaalista suvereniteettia.

EU toteutti vuonna 2021 tutkimuksen, jonka erityisenä tavoitteena oli selvittää, miten avoin lähdekoodi edistää teknologista riippumattomuutta, kilpailukykyä ja

innovaatioita EU-alueella. Tutkimusten perusteella EU:ssa suositellaan avoimen lähdekoodin käytön lisäämistä julkishallinnossa, mikä voi auttaa vähentämään omistuksen kokonaiskustannuksia, välttämään toimittajaloukkutilanteita sekä parantamaan digitaalista suvereniteettia.

Alla on kuvattu vielä tutkimustyön keskeiset huomiot.

- Teknologinen riippumattomuus: avoin lähdekoodi vähentää riippuvuutta ulkomaisista toimittajista.
- Kilpailukyky: avoin lähdekoodi edistää kilpailua ja vähentää pääsyesteitä markkinoille.
- Innovaatiot: avoin lähdekoodi mahdollistaa nopeamman innovaation, koska sen avulla yritykset ja kehittäjät voivat hyödyntää olemassa olevia ratkaisuja ja rakentaa niiden päälle.

Raportin mukaan avoimen lähdekoodin panos Euroopan unionin bruttokansantuotteeseen on huomattava. Avoimen lähdekoodin arvioidaan tuottavan jopa 100 miljardia euroa lisäarvoa EU-alueen talouteen tulevina vuosina, jos investoinnit kasvaisivat. (Blind et al. 2021)

Avoimen lähdekoodin hyödyntämisen mallit

Avoimen lähdekoodin kehitys on laaja käsite. Se voi tarkoittaa avoimen lähdekoodin hyödyntämistä omassa kehityksessä tai oman lähdekoodin jakamista avoimena. Se voi tarkoittaa yksityisen henkilön tekemän ratkaisun tai avoimeksi lähdekoodiksi avatun ison organisaation ylläpitämän tuoteratkaisun hyödyntämistä omassa kehityksessä. Hyödyntäminen voi olla suoraviivaista avoinna olevan lähdekoodin hyödyntämistä tai omaa ratkaisua voidaan toteuttaa osana avoimen lähdekoodin yhteisöä.

Säätiöpohjainen hallinta

Säätiöpohjainen avoimen lähdekoodin hallinta on yksi merkittävä tapa, jolla ylläpito ja hallinta toteutetaan. Esimerkkejä säätiöpohjaisesta hallinnoinnista ovat Eclipse Org, Linux Foundation sekä Apache Foundation. Säätiöpohjaisessa hallintatavassa rahoittajia pyritään aktiivisesti etsimään myös yksityisen sektorin toimijoista, joille ratkaisu voisi olla hyödyllinen. Tyypillistä säätiöpohjaisesti rahoitettaville ratkaisuille on niiden geneerinen luonne, mikä mahdollistaa ratkaisun hyödyntämisen mahdollisimman laajasti ja toimialariippumattomasti.

Yhteisöpohjainen hallinnointi

Avoimen lähdekoodin ympärille voidaan myös rakentaa yhteisö, missä jäsenet ovat sitoutuneet yhteisesti kehittämään ratkaisua eteenpäin. Tyypillisesti jäsenet myös rahoittavat kehitystä ja yhteisön toimintaa. Toimintaan on myös mahdollista hakea ulkopuolista rahoitusta, mikäli voidaan osoittaa ratkaisun tarjoamat hyödyt laajasti elinkeinoelämän ja laajasti eri toimialojen kehitykseen.

Hallitaan avointa lähdekoodia sitten säätiön tai yhteisöpohjaisen hallinnoinnin periaatteilla, mallin tarjoamat tukitoimet ratkaisun kehittämiselle ja kehitysyhteisön jäsenille ovat olennainen lisäarvo. Tukitoimet erottavatkin avoimessa lähdekoodissa yksityiset julkaisut yhteisö- tai säätiöpohjaisesta ratkaisujen kehittämisestä, joissa on tyypillisesti toimiva hallintopohja.

Tukitoimet sisältävät mm. seuraavia tehtäviä:

- Kehittäjäyhteisön tuki kullekin osallistuvalle taholle.
- Teknisen ekosysteemin kehitysyhteisön tuki (tekninen kehitysympäristö versionhallintoineen).
- Yhteisistä hallintomalleista sopiminen (projektien hallintaa koskevat periaatteet, menettelytavat, jotka edesauttavat ylläpitämään laadunvalvontastandardeja).
- Laaduntarkkailuprosessit.
- Immateriaalioikeuksien sekä lisenssien hallinta.
- Pitkäaikainen tuki ja ylläpidon varmistaminen tuotteelle.

Avoimen lähdekoodin ratkaisulle rahoitus on oleellista, kun ratkaisua toteutetaan yhteisömallilla ja pyritään saavuttamaan pitkäikäinen ja luotettava ratkaisu. Monet avoimen lähdekoodin organisaatiot sekä yhteisöt pyrkivätkin tuottamaan maksullisia lisäarvopalveluita ilmaisen toteutuksen rinnalle rahoitusmekanismeina, kuten konsultaatiota, lisäosia, SaaS-palveluita, koulutuksia sekä sertifiointeja. (COSS ry haastattelu 2024)

Yritykset myös usein hyödyntävät avoimen lähdekoodin tuotteita omien tuotteiden keskeisenä osana. Yritysten liiketoiminta saattaa näin olla merkittävästi riippuvainen kyseisestä avoimen lähdekoodin ratkaisusta. Toimiessaan näin yritykset pyrkivät osallistumaan aktiivisesti yhteisön toimintaan, jotta ne voivat vaikuttaa päätöksentekoon, kehitystyön painopisteisiin ja saavat yhteisön tuen lähdekoodin hyödyntämiseen (riskien hallinta).

Joskus yritykset perustavat itse avoimen lähdekoodin yhteisöjä. Silloin ne saattavat avata joidenkin keskeisten palveluiden tai tuotteiden ohjelmistoja tai erityisesti niiden osia avoimeksi. Samalla, kun ratkaisu avataan myös muiden hyödynnettäväksi, sen ympärille pyritään aktivoimaan aktiivinen kehitysyhteisö, joka kiihdyttää ratkaisun kehitystyötä ja toisaalta tuottaa uusia innovaatioita. Yritys luonnollisesti itse jatkaa avoimen yhteisön toiminnassa vahvana toimijana, jolloin sillä on hyvä näkymä ja hallinta sen kehityssuuntiin.

Yllä kuvatuissa tilanteissa (osallistuminen avoimen lähdekoodin yhteisöön tai sellaisen perustaminen) toiminnan tulisi perustua tarkkaan harkittuun avoimen lähdekoodin hyödyntämisen strategiaan. Strategiassa yritys määrittelee tarkkaan, minkälaisia hyötyjä se pyrkii saavuttamaan, minkälaisia avoimen koodin lisenssejä käyttämään ja millaisia välttämään. Yritys pyrkii myös strategian avulla varmistamaan tämän toiminnan tuottaman liiketoiminnallisen hyödyn, ja tunnistamaan kuinka toiminta parantaa kilpailukykyä. Tämä voi tapahtua esimerkiksi avaamalla joitakin ydinteknologioita avoimen lähdekoodin yhteisön kehitettäväksi, mutta kuitenkin säilyttämällä näiden päällä olevia liiketoimintakriittisiä lisäarvokerroksia. (Linux Foundation 2024)

Räätälöity toteutus

Räätälöitynä valmistettu ohjelmisto kehitetään ja suunnitellaan yleisesti tiettyä yritystä, organisaatiota tai käyttötarkoitusta varten. Toisin kuin valmiit, yleiseen käyttöön tarkoitetut tuoteratkaisut, räätälöity ohjelmisto vastaa tarkasti asiakkaan erityisiä vaatimuksia ja tarpeita. Se rakennetaan usein tyhjästä tai sen kehittämisessä hyödynnetään olemassa olevia ohjelmistokomponentteja, jotta se sopii täydellisesti käyttäjän prosesseihin, tavoitteisiin ja toimintaympäristöön.

Räätälöity toteutusmalli tarjoaa pääsääntöisesti organisaatiolle vahvan hallinnan ohjelmiston tekijänoikeuksiin sekä ohjelmistokoodiin.

Räätälöity ratkaisu rakennetaan vastaamaan tarkasti oman organisaation prosesseja sekä vaatimuksia. Yleensä tällöin on kyseessä erityinen tarve, joka ei noudattele useiden organisaation täysin samanlaisia tarpeita. Usein räätälöityä toteutusmallia ei käytetä tilanteissa, joissa kehityskohteena oleva ratkaisu on vahvasti määritelty ja standardoitu. Tämänkaltainen tilanne voisi mieluummin ohjata markkinoille syntyneiden tuoteratkaisujen käyttämiseen tai yhteiskehittämiseen avoimen lähdekoodin yhteisömallilla.

Tiedonvaihtopalvelimen osalta vaatimukset ja toiminnallisuudet pyritään määrittämään Euroopan tasolla yhtenäisiksi, joten räätälöidyn ratkaisun kehittäminen ei lähtökohtaisesti näyttäydy soveltuvimpana vaihtoehtona. Tiedonvaihtopalvelimen toiminta ja tuki erilaisille toiminnoille on kuitenkin kaikille sama. Tiedonvaihtopalvelimen ei myöskään tarvitse integroitua paikallisesti erilaisiin tietorajapintoihin, vaan sen kommunikointi tapahtuu aina valmiiksi määritellyillä tavoille toisten tiedonvaihtopalvelimien tai C-ITS-keskusyksiköiden kanssa. Toisaalta, jos tiedonvaihtopalvelimen osalta tunnistetaan selkeitä omia kansallisia räätälöintitarpeita, mihin valmiit tuotteet tai ratkaisut ei pysty vastaamaan, voi räätälöinti tuoda organisaatiokohtaista hyötyä.

7.7.2 Räätälöity toteutus avoimen lähdekoodin pohjalta

Yleinen tapa nykypäivänä oman räätälöidyn kehityksen osalta on käyttää kehitystyössä pohjalla avointa lähdekoodia, mikäli avoimessa lähdekoodissa käytetty lisensointi mahdollistaa tämän. Tätä mallia yleisesti avoimen lähdekoodin yhteisöissä kutsutaan ”forkkaukseksi”. Siinä avoimen lähdekoodin toteutuksesta irrotetaan lähdekoodin sen hetkinen versio omaan kehityshaaraansa.

Avoimen lähdekoodin hyödyntämiseen omassa räätälöidyssä toteutuksessa voi olla monia erilaisia motiiveja.

Yksityinen toimija voi lähteä toteuttamaan itselleen tuoteratkaisua ja aiheeseen liittyen tunnistetaan avoimen lähdekoodin yhteisö, jonka kehittämä ratkaisu on lähellä omaa kehitettävää tuotetta tai tarjoaa omaan tuoteratkaisuun edes joitakin valmiita osia. Näissä tilanteissa avoimen lähdekoodin käytön motiivina toimii useimmiten taloudellinen hyöty. Tarjolla ollut avoin koodi voi nopeuttaa tuotteen kehitysaikaa merkittävästi ja saattaa tuottaa myös hyötyä tuotteen jatkokehityksessä ja elinkaaren hallinnassa. Yrityksen oman tuotteen osio, joka on toteutettu avointa lähdekoodia hyödyntäen saattaa kehittyä ”itsekseen” avoimen lähdekoodin yhteisön toimesta, joka tekee siihen uusia ominaisuuksia, huolehtii sen tietoturvasta tai päivittää sitä aina uusien vaatimuksien mukaiseksi (esim. standardit).

Tähän toimintaan liittyy myös jo edellisessä alaluvussa mainittu riski. Jos organisaatio vain ottaa jonkun ajan hetken avoimen lähdekoodin ratkaisun koodin oman ratkaisun pohjalle, eikä aio mitenkään osallistua aktiivisesti yhteisön toimintaan, se ottaa riskin. Organisaatiolla ei olisi tällaisessa tapauksessa näkymää avoimen lähdekoodin kehitykseen, siihen liittyvään päätöksentekoon kehitystyön suunnista, eikä se saisi yhteisöltä tukea avoimessa koodissa tunnistettuihin ongelmiin. Aktiivinen osallistuminen avoimen lähdekoodin yhteisön kehitystyöhön myös varmistaa, että organisaatiolla on tarvittava osaaminen hyödynnettävästä

lähdekoodista. Näiden riskien suuruus vaihtelee suuresti riippuen hyödynnettävän avoimen lähdekoodin yhteisön ja sen toteuttamien ratkaisujen kypsyydestä.

Edellä mainitut seikat johtavat toiseen esimerkkiin ”forkkauksesta” eli olemassa olevan lähdekoodin hyödyntämisestä. Tässä esimerkissä organisaatio tunnistaa oman kehitettävän tuotteen näkökulmasta hyödyllisen avoimen lähdekoodin yhteisön ja ottaa sen tuottaman ratkaisun (tai osan siitä) oman ratkaisun kehityksen pohjalle tai osaksi. Organisaatio lähtee kehittämään tämän pohjalle esimerkiksi omaa kaupallista tuotetta ja alkaa kehittämään omia markkinoilla erottautumiseen tarvittavia liiketoimintakerroksia. Samaan aikaan organisaatio kuitenkin osallistuu myös oman tuotteen hyödyntämän ratkaisun avoimen yhteisön toimintaan, jotta se voi vaikuttaa sen kehityssuuntiin ja varmistaa myös, että sillä on riittävä osaaminen sen hyödyntämiseen.

Kolmas esimerkki sisältää ajatuksen, jossa perustamisesta saakka avoimen lähdekoodin yhteisössä toimiva jäsen on aluksi vahvasti mukana kehittämässä yhteisön mukana ratkaisua, mutta kehitystyön kuluessa haluaa lähteä kehittämään yhteisön toteuttaman ratkaisun pohjalta myös omaa ratkaisua. Tähän päätökseen voi olla syynä eriävät näkemykset yhteisön sisällä ratkaisun kehityksen suunnasta tai yhteisön jäsenen tunnistamat omat tarpeet, jotka eivät ole linjassa muiden yhteisön jäsenien kanssa. Mikäli organisaatio ei jatka enää avoimen yhteisön toiminnassa tulee kuvaan jo esitetyt riskit: näkymä ja vaikutusmahdollisuudet yhteisön tekemisiin ja yhteisön jäsenten tuki lakkaavat. Tässäkin mallissa yhteistyö alkuperäisen lähdekoodin ylläpitäjän kanssa voi olla edelleen kuitenkin mahdollista. Organisaatio voi jatkaa edelleen yhteisön jäsenenä, mikäli oman kehityshaaran lisäksi sitoutuu myös yhteisön sääntöihin, kehityslinjoihin ja panostukseen.

Yllä kuvatun kaltaisesta kehityshaaran eriyttämisestä on olemassa onnistuneita esimerkkejä kuten LibreOffice, joka eriytettiin OpenOfficestä, ja on nykyään aktiivisempi ja yleisemmin käytetty versio. Samoin io.js, joka oli alun perin Node.js:stä irrotettu haara, mutta myöhemmin projektit yhdistyivät takaisin Node.js-projektiksi.

7.7.3 Tuotehankinta

Tuotepohjainen ohjelmistoratkaisu voi olla nopeampi, edullisempi ja vakaampi vaihtoehto organisaatioille, jotka eivät tarvitse räätälöityjä ratkaisuja erikoistarpeisiin. Se tarjoaa valmiita päivityksiä, laajaa tukea ja dokumentaatiota, sekä skaalautuvuutta, mikä tekee siitä houkuttelevan valinnan.

Kääntöpuolena tuotepohjaisissa ratkaisuissa on, että ne eivät aina vastaa kaikkiin erityistarpeisiin. Ne voivat rajoittaa räätälöintimahdollisuuksia, aiheuttaa riippuvuutta toimittajasta ja johtaa tarpeettomiin ominaisuuksiin tai lisäominaisuuksien osalta kasvaviin kustannuksiin.

Valmiina kaupallisina ohjelmistoina saatavilla olevat tuotepohjaiset ratkaisut ovat usein kokonaiskustannuksiltaan edullisempia kuin omat räätälöidyt ohjelmistototeutukset. Tuotepohjaisissa ratkaisuissa tuotteen käyttöönotto on yleensä merkittävästi kustannuksiltaan edullisempi, vaikka se sisältäisi kohdekohtaista räätälöintiä esimerkiksi tuotteen lokalisoinnin tai ympäröivien tietolähteiden ja järjestelmien integroinnin suhteen.

Käyttöönottoa seuraa yleensä sopimuskauden aikaiset palvelumaksut. Palvelumaksut tuottavat ratkaisun taloudelliseen hallintaan merkittävästi parempaa ennustettavuutta kuin oma räätälöity toteutus. Tyypillisesti palvelumaksuihin sisältyy tuotteeseen tehtävät välttämättömät tietoturvapäivitykset. Päivitykset sisältävät myös tyypillisesti välttämättömät standardien päivityksiin liittyvät muutokset.

Mikäli tuotepohjaista ratkaisua halutaan kehittää ostajaorganisaation halujen mukaisesti, niin tämä ei välttämättä ole aina mahdollista. Usein kuitenkin tuotteen tarjoajaorganisaatio saattaa olla valmis kehittämään tuotteeseen asiakaskohtaisia ominaisuuksia palvelusopimuksessa yhteisesti sovitulla tuntilaskutushinnalla. Tämä ei kaupallisesti käytännössä eroa merkittävästi omassa omistuksessa olevan räätälöidyn ohjelmiston vaihtoehtoon verrattuna. Oma räätälöity tuote tehdään alun perinkin ohjelmistokumppanin kanssa maksullisesti ja jos sitä halutaan elinkaaren aikana päivittää tai muokata, niin ohjelmistokumppanille maksetaan muutoksista tyypillisesti jonkun puitesopimuksen puitteissa sovitun tuntilaskutushinnan mukaisesti. Toki omassa omistuksessa olevaan räätälöityyn ohjelmistoon tehtävien muutosten toteutus on mahdollista kilpailuttaa, kun tuotepohjaiseen ohjelmistoon ainut mahdollinen toteuttaja on tuotteen omistaja.

Tiedonvaihtopalvelimiin liittyen tuotepohjaisia tiedonvaihtopalvelimia ei markkinoilla ole vielä juurikaan olemassa. Tämä johtuu siitä syystä, että markkinoilla ei ole ollut sellaisille tähän saakka juurikaan tarvetta (ei ole siis vielä markkinoita). Kun C-Roads-määrittelyt etenevät pitkän kantaman tiedonsiirron IP-pohjaisten ratkaisujen osalta ja jäsenmaihin rakentuvia kansallisia C-ITS-palvelutoteutuksia aletaan yhdistämään toisiinsa, niin markkinoille alkaa todennäköisesti syntymään myös tuotepohjaisia ratkaisuita myös tähän tarpeeseen.

Tällä hetkellä lähimpänä tuotepohjaisia vaihtoja markkinoilla on Monotchin TLEX-tuote, joka sisältää myös tiedonvaihtopalvelinosuuden. Suomessa TLEX-tuotetta on hyödynnetty Tampereen kaupungin ja Fintraffic Tie Oy:n NordicWay3-kokeilussa, ja tuotteen käyttöä on jatkettu osittain myös tämän jälkeen. Samassa yhteydessä toteutettiin TLEX-tuotteen ja norjalaisen avoimen lähdekoodin tiedonvaihtopalvelimen välinen integraatiopilotti, jossa testattiin näiden välisen yhteyden toimintaa.

TLEX-järjestelmän kehitys on aloitettu Hollannissa tilanteessa, jolloin C-Roads-spesifikaatiot pitkän kantaman tiedonsiirtoon eivät olleet valmiita. Tästä syystä TLEX ei ole täysin standardien mukainen, ja Monotchin mukaan he odottavat määrittelyjen valmistumista, ennen mahdollisten uusien C-Roads-spesifikaatioihin liittyvien ominaisuuksien kehittämistä. (Monotch haastattelu 2024)

7.8 Tiedonvaihtopalvelimen toteutuksen pohdinta

Tiedonvaihtopalvelimen toteutusvaihtoehtoja esiteltiin edellisessä luvussa 7.7. Luvussa tuotiin monipuolisesti esille useita eri tapoja toteuttaa tiedonvaihtopalvelin. Alla on lyhyesti käsitelty kutakin toteutusmahdollisuutta suomalaisen tiedonvaihtopalvelimen toteutuksen näkökulmasta.

Alla on lueteltu muutamia rajauksia ja lähtöoletuksia tähän tarkasteluun.

- Suomeen ei ole välttämätöntä toteuttaa enempää kuin yksi tiedonvaihtopalvelin, jolla hoidetaan tulevaisuudessa yhteiseurooppalainen maiden välisten C-ITS-palveluiden välinen tiedonsiirto. Yhtenä mahdollisuutena voidaan nähdä

myös (erityisesti alkuvaiheessa) liittyminen suomalaisista C-ITS-keskusyksiköistä jonkun toisen maan tiedonvaihtopalvelimeen,

- Suomalainen tiedonvaihtopalvelin voi jatkossa toimia myös Suomeen mahdollisesti syntyvien useampien C-ITS-keskusyksiköiden yhdysliikennepisteenä.
- Todennäköisintä on, että suomalaisen tiedonvaihtopalvelimen operoijana toimii Fintraffic Tie Oy (Kotilainen et al. 2023).
- Tiedonvaihtopalvelimen toteutus ei välttämättä ole aikataulullisesti kiireellisin osuus C-ITS-järjestelmän toteutusta (erityisesti niin kauan, kun palvelut tuotetaan loppukäyttäjille matkaviestinverkkojen yli mobiilisovellusten avulla).

Taulukossa 12 on käsitelty tiedonvaihtopalvelimen hankintamallien hyötyjä ja haittoja.

Taulukko 12. Tiedonvaihtopalvelin erilaisten toteutusvaihtoehtojen vertailu.

Oma räätälöity ohjelmistototeutus	
+ Kehityksen joustavuus + Riippumattomuus + Ei mahdollisesti hankalaa tuotekilpailutusta (ehkä asiantuntijaresurssien minikilpailutus puitesopimusten sisällä)	- Hinta - Kallis elinkaarenhallinta - Vaatii käyttöpalveluiden hankinnan palvelun toimintaympäristön osalta (palvelinsali/pilvipalveluympäristö, hallinta-, valvonta- ja vianselvityspalvelut erillisenä hankintana - Vaikeasti ennakoitavat kehitystarpeet, joihin kaikkiin tulee hankkia ulkopuolista asiantuntijatyötä (ympäristön aiheuttamat muutokset, kuten komission vaatimukset, käytettyjen teknologioiden tuen loppuminen, jatkuvaan C-ITS-järjestelmään kasvuun sopeutuminen)
Räätälöity ohjelmistototeutus avoimen lähdekoodin pohjalle	
+ Kustannussäästöt ensimmäisessä toteutusversiossa avoimen koodin hyödyntämisen myötä + Kehityksen joustavuus	- Hyödynnettävään avoimeen lähdekoodiin liittyvät riskit (avoimessa koodissa mahdollisesti piilevät virheet ja tietoturva-aukot voi olla hankala löytää, vikatilanteissa työllistää paljon, saako varsinaiselta kehittäjältä apua? - Haaste ottaa haltuun avoin koodi (tekijöillä ei ole mitään kokemusta aikaisemmin toteutetusta osuudesta, tutustumiseen kuluu aikaa, koodaajien yleisesti tunnistettu haluttomuus hyödyntää muiden tekemää)

	- Kallis elinkaarenhallinta, mahdollisia hyötyjä saadaan avoimen koodin kehittymisen avulla - Yllä olevat riskit konkretisoituvat erityisesti, mikäli avoimen yhteisön toimintaan ei osallistuta aktiivisesti. - Raskas käyttöpalveluympäristön kustannus (palvelinsali/pilvipalveluympäristö, tietoturvapalvelut, hallinta-, valvonta- ja vianselvityspalvelut erillisenä hankintana) - Vaikeasti ennakoitavat kehitystarpeet
Avoimen lähdekoodin yhteisökehittäminen	
+ Kehitystyöhön osallistuu useampia rahoittajia + Mahdollisuus saada EU-tukia + Kehityksen joustavuus (yhteisössä voidaan päättää suunnasta, toisaalta voidaan myös alkaa kehittämään omaa haaraa tuotteesta) + Kehitysyhteisö tuottaa tukea jäsenilleen toteutetun ympäristön osalta	- Yhteisön perustamisen hallinnollinen kuorma (hallintomallit, yhteisen maalin määrittely, rahoituksesta sopiminen, yhteisten käytännön toimintamallien sopiminen) - Kehitysaikaiset näkemyserot kehityksen suunnassa - Raskas käyttöpalveluympäristön kustannus (palvelimet, pilvet, tietoliikenne, tietoturva, hallinta, valvonta, reagointi- ja vianselvitys)
Tuotehankinta	
+ Alhaisemmat aloituskustannukset + Nopeampi käyttöönotto + Tuote kehittyy aiheeseen liittyvien uusien EU-vaatimusten osalta automaattisesti (kuuluu yleensä palveluhintaan ja voi vaatia kilpailutuksessa) + Palveluhintaan kuuluu toimittajan hallinnoima käyttöpalveluympäristö (palvelimet, pilvet, tietoliikenne, tietoturva, hallinta, valvonta, reagointi- ja vianselvitys)	- Kilpailutusprosessi - Sopimuskausien vaihtumisen mahdollisesti aiheuttamat haasteet tuotteen vaihdosta - Ei niin joustava kehitys (jos omia tarpeita) - Toimittajaloukku erityisesti, jos ratkaisu kehittyy suuntaan, jossa siitä syntyy vahvasti oma räätälöity toteutus, joka on hankala korvata markkinoilla olemassa olevilla tuotteilla, toinen riski on suuri määrä räätälöityjä integraatioita ulkoisiin järjestelmiin, vähiten riskiä, jos ratkaisu on valmiiksi vaatimuksien osalta standardoitu, eikä sitä räätälöidä merkittävästi

Yhteenvetona voidaan todeta, että tiedonvaihtopalvelin on pitkälle standardoitu ratkaisu C-Roadsin asettamien vaatimusten myötä. Sen toiminnallisuudet ovat samanlaiset kaikkialla, missä sitä käytetään osana eurooppalaista C-ITS-palvelutoteutusten arkkitehtuuria. Tiedonvaihtopalvelimen käyttöönotto ei vaadi paikallista lokalisointia tai ulkoisiin järjestelmiin tehtävää räätälöityä integraatiota. Tätä taustaa vasten ei ole välttämättä kovin hyvin perusteltua lähteä toteuttamaan täysin omaa suomalaista versiota tyhjästä.

Yllä kuvatun myötä vahvoina vaihtoehtoina tiedonvaihtopalvelimen kehitykselle jää joko tuotehankinta tai avoimen lähdekoodin hyödyntäminen. Näissä kummassakin ratkaisussa Suomen on syytä toteuttaa myös strategista suunnittelua liittyen myös tämän ratkaisun toteutustapaan (ja laajemminkin C-ITS-toimialan kehitykseen) liittyen.

Tuoteratkaisuihin liittyen suomalaisille yrityksille mahdollisesti syntyvät tuote- ja palvelumarkkinat kannattaa huomioida osana tuotteen hankintaa. Avoimen lähdekoodin hyödyntämiseen tai yhteisön toimintaan liittyen on tärkeää tehdä tähän toimintaan liittyvä strateginen suunnittelu. Suunnittelun avulla pyritään vastaamaan kysymyksiin, miten avointa lähdekoodia hyödynnetään, minkälaisia lisenssejä käytetään, mikä on oma rooli avoimen yhteisön toiminnassa, kuinka varmistetaan, että avoimen yhteisön kehityssuuntiin ja päätöksentekoon päästään vaikuttamaan, kuinka varmistetaan oma osaaminen ja miten samalla mahdollistetaan yksityisen sektorin liiketoimintamahdollisuuksia.

Avoin yhteisötoiminta (esim. yhteispohjoismainen) voisi myös tarjota merkittäviä mahdollisuuksia suomalaiselle (ja pohjoismaiselle) yksityissektorille. Tämä vaatisi julkishallinnolta vahvaa yksityisen sektorin huomioimista osana avoimen lähdekoodin kehitystyötä. Tämä voisi tarkoittaa yksityissektorin kanssa yhteistyössä tehtävää strategista suunnittelua sen suhteen, mitä todellisuudessa avoimessa yhteisössä olisi järkevää kehittää (esimerkiksi keskeisiä ratkaisujen ydinkomponentteja) ja minkälaisia lisäarvokerroksia voitaisiin jättää yksityisen sektorin toteutettavaksi. Tällöin yksityissektori hyötyisi merkittävästi julkishallinnon kehitystyöstä osana avointa yhteisöä, se pystyisi myös osallistumaan avoimen yhteisön toimintaan (mikä hyödyttäisi julkista sektoria) ja samalla yksityiselle sektorille voisi syntyä merkittäviä liiketoimintamahdollisuuksia, kun se voisi tuottaa avoimen yhteisön kehittämien ydinkomponenttien päälle omia lisäarvokerroksia, tuotteistaa niiden päälle kaupallisia ratkaisuja ja tuottaa niille tukipalveluita.

Edellisessä kappaleessa kuvatut keinot tulisi olla keskeinen osa avoimen lähdekoodin yhteisössä toimimiseen liittyvää avoimen lähdekoodin liiketoimintastrategista ajattelua ja suunnittelua. Keinoilla pyritään varmistamaan, että suomalaisella kehitystyöllä ja investoinneilla kehitetään samanaikaisesti suomalaista liikennejärjestelmää, paikallista liiketoimintaympäristöä, joka voisi mahdollistaa jopa kansainvälistyvät suomalaiset innovaatiot.

8 Yksityisyyden suoja C-ITS-palveluissa

Henkilötietojen suoja ja yksityiselämän kunnioittaminen ovat eurooppalaisia perusoikeuksia. Euroopan parlamentti on aina korostanut tarvetta säilyttää tasapaino turvallisuuden lisäämisen sekä ihmisoikeuksien, myös tietosuojan ja yksityisyyden, turvaamisen välillä. (Faktatietoja Euroopan unionista, 2025).

Myös C-ITS-palveluissa yksityisyyden suoja ja tietosuoja ovat toisiaan täydentäviä konsepteja. Yksityisyyden suoja keskittyy yksilön oikeuksiin ja valinnanvapauteen omien tietojensa suhteen. Se painottaa yksityiselämän suojaa ja itsemääräämisoikeutta ja vastaa kysymykseen "mitä tietoja kerätään ja miksi?" Tietosuoja puolestaan painottaa lainsäädännön mukaisesti kerättyjen tietojen teknistä suojaamista ja turvallista käsittelyä. Se määrittelee konkreettiset toimenpiteet tietojen suojaamiseksi ja painottaa tietojen turvallista käsittelyä ja säilytystä vastaten kysymykseen "miten tietoja käsitellään ja suojataan?"

8.1 Yksityisyyden- ja tietosuojan periaatteet

EU:n yleinen tietosuoja-asetus (EU 2016/679, GDPR), tuli voimaan toukokuussa 2016 ja sitä alettiin soveltamaan toukokuussa 2018. Se lujittaa kansalaisten oikeuksia ja yksinkertaistaa yrityksiin sovellettavia sääntöjä digitalisaation aikakaudella. Sääntöjen tarkoituksena on suojella kaikkia EU:n kansalaisia yksityisyyden ja tietoturvan loukkauksilta yhä tietointensiivisemmässä maailmassa ja samalla luoda yrityksille entistä selkeämpi ja yhtenäisempi toimintakehys. Suomessa Tietosuojalaki (1050/2018) täsmentää ja täydentää GDPR:ää ja sen kansallista soveltamista.

GDPR takaa rekisteröidyille tiettyjä oikeuksia. Henkilöillä on oikeus saada tietoa siitä, miten heidän henkilötietojaan käsitellään ja heillä on oikeus päästä käsiksi tietoihin, joita yrityksellä tai organisaatiolla heistä on. Jokaisella on oikeus henkilötietojensa suojaan. Se on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä, samalla kun suojataan yksilöiden yksityisyyttä ja varmistetaan heidän oikeuksiensa kunnioittaminen.

Henkilötietoja ovat tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Arvioitaessa onko tieto henkilötietoa vai ei, on mahdollinen tietojen yhdisteltävyys keskeinen konsepti. Tämä tarkoittaa, että esimerkiksi C-ITS-viestipaketit, jotka ovat yhdistettävissä tiettyyn ajoneuvoon, joka on yhdistettävissä tiettyyn runkonumeroon, joka on yhdistettävissä tiettyyn rekisterinumeroon, joka on yhdistettävissä tiettyyn ajoneuvon käyttömaksun lähetysosoitteeseen, muuttuu henkilötiedoksi, jota tulee kohdella henkilötietojen käsittelyä määräävän lainsäädännön mukaisesti. Näin ollen henkilötietoa saattaa muodostua hyvinkin yllättävissä yhteyksissä.

8.1.1 Tietosuojan periaatteet

Tietosuojaperiaatteita on noudatettava aina, kun käsitellään henkilötietoja ja niitä on noudatettava koko henkilötietojen käsittelyn elinkaaren ajan. Rekisterinpitäjän on myös pystyttävä osoittamaan, että tietosuojaperiaatteet toteutuvat tehokkaasti henkilötietojen käsittelyssä.

Henkilötietojen käsittely

Tietosuojaperiaatteiden (periaatteet suluissa) mukaan henkilötietoja on

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (Lainmukaisuus, asianmukaisuus ja läpinäkyvyys)
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten (Käyttötarkoitussidonnaisuus)
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden (Tietojen minimointi)
- päivitettävä aina tarvittaessa. Epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä (Tietojen täsmällisyys)
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten (Säilytyksen rajoittaminen)
- käsiteltävä luottamuksellisesti ja turvallisesti (Luottamuksellisuus ja turvallisuus).

Jotta henkilötietojen käsittely olisi lainmukaista, sille on oltava lainsäädäntöön sisältyvä käsittelyperuste. Peruste on määritettävä ennen käsittelyn aloittamista. Kun henkilötietojen käsittely sidotaan johonkin käsittelyperusteeseen, perustetta ei voi enää vaihtaa toiseen. Käsittelyperuste vaikuttaa merkittävästi siihen, mitä oikeuksia rekisteröidyllä on suhteessa rekisterinpitäjään. Rekisterinpitäjän on myös pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä. Osoitusvelvollisuuden tarkoituksena on näyttää, miten rekisterinpitäjä kunnioittaa rekisteröityjen eli henkilötietojen käsittelyn kohteena olevien tietosuojaa.

Henkilötietojen käsittelyperuste

Henkilötietojen käsittelyperuste voi olla:

- Rekisteröidyn *suostumus* eli vapaaehtoinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.
- *Sopimus*, kun henkilö on osapuolena sopimuksessa esim. tilatessaan tavaroita verkosta, yritys voi käsitellä hänen osoitetietojaan.
- *Lakisääteinen velvoite*, joka perustuu EU:n tai jonkin jäsenvaltion lakiin.
- *Elintärkeiden etujen suojaaminen* esim. tilanteissa, joissa on kyse rekisteröidyn tai jonkun toisen henkilön elämästä, kuolemasta tai vakavasta uhasta terveydelle.
- *Yleistä etua* koskeva tehtävä tai julkinen valta, kun yleinen etu tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen sitä edellyttää. Tämä voi toimia käsittelyperusteena niin yksityisellä kuin julkisella sektorilla tilanteissa, joissa on kysymys EU:n tai jäsenvaltion yleisestä edusta tai julkisesta vallasta.
- Rekisterinpitäjän *oikeutettu etu* toteutuu esimerkiksi silloin, kun rekisterinpitäjän ja rekisteröidyn välillä on jokin merkityksellinen suhde. Se tarkoittaa, että rekisteröity on esimerkiksi rekisterinpitäjän asiakas tai alainen. Oikeutettu etu edellyttää rekisterinpitäjän omaa arviointia tasapainotestin avulla. Julkisella puolella oikeutettua etua ei yleensä katsota soveliaaksi

käsittelyperusteeksi, koska muut perusteet, kuten lakisääteiset tehtävät tai yleinen etu, ovat yleensä selkeämpiä ja sopivat paremmin julkissektorin säädösmuotoiseen toimintaan. (Tietosuojavaltuutetun toimisto, n.d., 'Käsittelyperusteet')

8.1.2 Riskienhallinta

Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyviä riskejä aina ennen kuin se ryhtyy käsittelemään henkilötietoja. Riskienarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Se on tarkoitettu jatkuvaksi riskien tunnistamisen ja hallitsemisen prosessiksi. Yksi työkalu riskien arviointiin on tietosuojaa koskeva vaikutustenarviointi, jota rekisterinpitäjä voi hyödyntää, kun se suunnittelee henkilötietoja käsitteleviä toimintoja. (Tietosuojavaltuutetun toimisto, n.d., 'Arvioi riskit')

Vaikutustenarvioinnissa kuvataan henkilötietojen käsittelyä, arvioidaan käsittelyn tarpeellisuutta, oikeasuhteisuutta ja henkilötietojen käsittelystä aiheutuvia riskejä sekä tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutustenarviointi on tehtävä, kun suunnitellaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille.

Vaikutustenarvioinnin tavoitteena on selvittää, onko jäljelle jäänyt riski oikeutettu ja hyväksyttävissä käsillä olevissa olosuhteissa. Vaikutustenarviointi auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, dokumentoinnissa ja osoittamisessa. (Tietosuojavaltuutetun toimisto, n.d., 'Arvioi riskit')

Riskin tunnistamisen merkitys korostuu erityisesti silloin, kun rekisterinpitäjä määrittää teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan tietosuojan toteutuminen henkilötietojen käsittelyssä. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstölle annettuja ohjeita tietosuojan toteuttamiseksi, omavalvonnan kautta tapahtuvaa käytönvalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta ja muita suojatoimenpiteitä.

Riskien arviointi on jatkuvaa toimintaa. Toimenpiteiden riittävyyttä suhteessa käsittelyyn liittyvään riskiin on arvioitava jatkuvasti ja päivitettävä tarvittaessa. Rekisterinpitäjällä on myös osoitusvelvollisuus riskiperusteisen lähestymistavan noudattamisesta.

8.1.3 Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle

C-ITS-viestejä muodostetaan ajoneuvoissa ja niitä lähetetään ajoneuvoihin, joten kansainvälisen ajoneuvoteollisuuden rooli tietojen käsittelijänä on huomioitava yksityisyyden suojan kannalta, jos tietoja käsitellään Euroopan talousalueen (ETA) ulkopuolella. Edellytyksenä henkilötietojen siirrolle ETA-alueen ulkopuolelle on, että henkilötietojen käsittelyn on oltava sallittua kyseisessä tilanteessa ja henkilötietojen siirroille on oltava EU:n yleisen tietosuoja-asetuksen (GDPR) V luvussa määritelty siirtoperuste. Siirtoperusteen tehokkuus ja täydentävien suojatoimien tarve on arvioitava tapauskohtaisesti.

Ensisijainen siirtoperuste on Euroopan komission antama tietosuojan riittävyyttä koskeva päätös (nk. riittävyyspäätös). Jos komissio on päättänyt, että kyseinen kolmas maa, alue, sektori tai kansainvälinen järjestö varmistaa riittävän tietosuojan tason, henkilötietoja voi siirtää suoraan riittävyyspäätöksen perusteella.

Jos riittävyyspäätöstä ei ole, on selvitettävä, voidaanko henkilötietoja siirtää muilla siirtoperusteilla, kuten vakiolausekkeilla tai yrityksiä koskevien sitovien sääntöjen perusteella. Jos henkilötietoja ei voida siirtää komission riittävyyspäätöksellä tai käyttämällä muita siirtoperusteita, voidaan vielä selvittää, onko henkilötietoja mahdollista siirtää erityistilanteita koskevan poikkeuksen perusteella. (Tietosuojavaltuutetun toimisto, n.d., 'Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle')

8.1.4 Siirtovaikutusten arviointi

Siirtovaikutusten arviointi (Transfer Impact Assessment, TIA) tarvitaan silloin, kun henkilötietoja siirretään Euroopan unionin (EU) tai Euroopan talousalueen (ETA) ulkopuolelle ja em. riittävyyspäätöstä ei ole. TIA:n avulla arvioidaan siirron laillisuutta ja varmistaudutaan siitä, että tiedonsiirron kohteena olevassa maassa on riittävä tietosuojan taso, joka vastaa esimerkiksi EU:n yleisen tietosuoja-asetuksen (GDPR) vaatimuksia.

GDPR ei nimenomaisesti vaadi TIA-arviointia erillisenä käsitteenä, mutta EU:n tietosuojaviranomaiset ja Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB) ovat korostaneet sen tärkeyttä osana GDPR:n V luvun täyttymistä. Erityisesti tilanteissa, joissa henkilötietoja siirretään EU- tai ETA-alueen ulkopuolelle ilman riittävyyspäätöstä, TIA nähdään osana asianmukaisten suojatoimenpiteiden käyttöönottoa ja riskienhallintaa. (Tietosuojavaltuutetun toimisto, n.d., 'Tiedonsiirtovälineitä täydentävät suojatoimet')

8.1.5 Rekisteröidyn informointi

Rekisteröityä tulee erityisesti informoida henkilötietojen käsittelyn tarkoituksista ja käsittelyn oikeusperusteesta. Jos henkilötietoja ei ole saatu rekisteröidyltä, tulee lisäksi ilmoittaa kyseessä olevat henkilötietoryhmät. Lisäksi rekisteröidylle on kerrottava läpinäkyvästi henkilötietojen vastaanottajat tai vastaanottajaryhmät, kansainvälisistä tiedonsiirroista, henkilötietojen säilytysaika, rekisteröidyn oikeuksista ja automaattisesta päätöksenteosta ja mahdollisesta jatkokäsittelystä ennen kyseistä käsittelyä. (EU 2016/679, 2016)

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai luvaton pääsy tietoihin.

Rekisterinpitäjällä on velvollisuus arvioida tapahtuman riskitaso ja sen mukaisesti dokumentoida tapahtuma ja ilmoittaa valvovalle viranomaiselle. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Ilmoitusta ei vaadita, jos on toteutettu tekniset ja organisatoriset suojatoimenpiteet, ja niitä on sovellettu henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin, tai rekisterinpitäjä on tehnyt jatkotoimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu. (Tietosuojavaltuutetun toimisto, n.d., Tietoturvaloukkaukset)

8.1.6 Rekisteröidyn oikeudet

Rekisteröidyllä on oikeus tarkastuspyynnön avulla saada tietoa käsiteltävistä henkilötiedoista ja niiden alkuperästä, käsittelyn tarkoituksista ja oikeusperusteesta, käsittelyn kohteena olevista henkilötietoryhmistä (jos tietoja ei ole saatu rekisteröidyltä), vastaanottajista tai vastaanottajaryhmistä, joille rekisteröidyn tietoja on luovutettu sekä henkilötietojen säilytysaika tai sen määrittämisperuste. Lisäksi rekisteröidyllä on oikeus pyytää henkilötietojensa oikaisemista, poistamista tai niiden käsittelyn rajoittamista sekä vastustaa niiden käsittelyä ja olla joutumatta automaattisen päätöksenteon kohteeksi. Rekisteröidyn tiedot on voitava siirtää toiselle rekisterinpitäjälle, jos se on teknisesti mahdollista.

Rekisteröity ei voi käyttää kaikkia oikeuksia kaikissa tilanteissa. Tilanteeseen vaikuttaa esimerkiksi se, millä perusteella henkilötietoja käsitellään. (Tietosuojavaltuutetun toimisto, n.d., Rekisteröidyn oikeudet)

8.1.7 Henkilötietojen anonymisointi ja pseudonymisointi

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa mm. nimen, osoitteen, henkilötunnuksen, auton rekisterinumeron, IP-osoitteen tai jonkin hänelle tunnusomaisen tekijän perusteella.

EU:n yleinen tietosuoja-asetus (EU 2016/679, GDPR) suojaa henkilötietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään. Tietojen säilytystavalla ei myöskään ole merkitystä. Tietoja voidaan säilyttää esimerkiksi IT-järjestelmässä, videovalvontajärjestelmässä tai paperiarkistossa. Niin pitkään, kun tietojen perusteella voi tunnistaa henkilön suoraan tai välillisesti tai tiedot voidaan palauttaa takaisin tunnistettavaan muotoon, ne ovat yhä henkilötietoja ja niihin sovelletaan GDPR:ää.

Yksityisyyden suojan tekniset ratkaisut voidaan jakaa (i) anonymisointiin ja (ii) pseudonymisointiin. Anonymisointi tarkoittaa pysyvää tunnistetietojen poistamista ja datan yhdistämistä ilman yksilöiviä tietoja. Tunnistamisen täytyy estyä peruuttamattomasti ja siten, että rekisterinpitäjä tai muu ulkopuolinen taho ei voi enää hallussaan olevilla tiedoilla muuttaa tietoja takaisin tunnistettaviksi. Anonymisoinnissa on otettava huomioon kaikki kohtuudella toteutettavissa olevat keinot, joiden avulla tiedot voitaisiin muuttaa takaisin tunnisteellisiksi. Rekisterinpitäjän on varauduttava myös siihen, että kerran tehty anonymisointi voi heiketä ajan ja teknisen kehityksen myötä. Voidaanko jokin tieto lopulta katsoa anonyymiksi vai ei, edellyttää tapauskohtaista arviointia. Henkilö voi olla tunnistettavissa muutenkin kuin nimen perusteella. Pelkästään nimien ja muiden yksilöintitietojen poistaminen ei aina tarkoita, että henkilörekisterin tiedot muuttuisivat anonyymeiksi. Anonymisoituja tietoja ei enää katsota henkilötiedoiksi, eikä niihin sovelleta tietosuojasäännöksiä. (Tietosuojavaltuutetun toimisto, n.d., Pseudonymisoidut ja anonymisoidut tiedot)

Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Esimerkiksi henkilötietojen koodaaminen on pseudonymisointia. Koodattuja tietoja ei voida yhdistää tiettyyn henkilöön ilman koodiavainta. Koodiavaimen haltija voi kuitenkin purkaa tietoaineiston salauksen ja tunnistaa uudelleen jokaisen rekisteröidyn.

C-ITS-ympäristössä pseudonymisointi tarkoittaa vaihtuvia tunnistetietoja ja linkityksen estoa eri palveluiden välillä. C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) perustuu tähän. Tästä esimerkkinä liikkuvan C-ITS-yksikön (ajoneuvo) viestinnän yksityisyyden suojaaminen. Viestin lähettäjä käyttää viestinnässä vaihtuvia valtuutuslippuja (AT, Authorization Ticket). Valtuutuslipulla vahvistetaan viestijän oikeus osallistua tiettyjen C-ITS-palveluiden (viestityypit) viestintään. Ne toimivat lyhytaikaisina varmenteita mahdollistaen viestinnän ilman, että laitteen tai ajoneuvon oikea identiteetti paljastuu. Koska tiedot ovat pseudonymisoitu, niiden avulla yksilö voidaan edelleen erottaa joukosta ja yhdistää eri tietoaineistoissa. Pseudonymisoidut tiedot ovat yhä henkilötietoja, ja niiden käsittelyssä on sovellettava tietosuojasäännöksiä.

EU:n C-ITS-turvatunnusten hallintajärjestelmässä PKI (Public Key Infrastructure) varmennus tarjoaa perustan viestien luotettavuudelle ja tietoturvalle. Teknisesti PKI-infrastruktuuria voidaan täydentää edistyneillä kryptografisilla menetelmillä, kuten nollatietotodistuksilla (Zero-Knowledge Proof), ryhmäallekirjoituksilla (Group Signature) ja sokkoallekirjoituksilla (Blind Signature). PKI-menetelmä jättää varmentajalle (certificate authority) mahdollisuuden ajoneuvon yksilöivään tunnistamisen tai ajoneuvo voidaan yhdistää, vaikka kamerakuvaan. Tällöin esimerkiksi ryhmäallekirjoitukset voivat laajentaa suojaa ja mahdollistaa ryhmän jäsenen anonymiteetin säilyttämisen viestinnässä. Tämä edistää viestien luotettavuutta ilman, että yksittäinen ajoneuvo voidaan suoraan tunnistaa (Yue et al. 2022). C-Roads-profiilispesifikaatiot ja ETSI:n spesifikaatiot keskittyvät kuitenkin edelleen perinteisempiin menetelmiin, ja tällaista lisäsuojaa ei ole vielä määritelty.

8.2 C-ITS-viestien yksityisyyden suojaa koskevat vaatimukset

EU:n delegoitua C-ITS-asetusehdotusta (C/2019/1789) ei hyväksytty EU:n parlamentin käsittelyssä 2019, joten tällä hetkellä C-ITS-palveluiden yhteydessä henkilötietojen suojaaminen ja käsittely on vahvasti sidoksissa yleiseen sekä kansalliseen että EU-tason sääntelyyn. Kyseisen asetusehdotuksen Liite 4 käsitteli erityisesti C-ITS-turvallisuuspolitiikkaa, mutta asetusehdotuksen uudelleen avaamisesta ja käsittelystä ei ole vielä tietoa. Hylätty asetusehdotus ja sen pohjalta tehdyt arvioinnit ovat kuitenkin toimineet tärkeänä lähtökohtana C-ITS-palveluiden määrittelyyn ja kehitykseen. Näin on myös yksityisyyden suojan osalta.

8.2.1 EU-tason vaatimukset

Keskeiset EU-tason sääntelymekanismit ovat:

EU:n yleinen tietosuoja-asetus (EU 2016/679, GDPR): Henkilötietojen käsittelyä EU:n jäsenmaissa säädellään GDPR:n nojalla. C-ITS:n yksityisyyden suojaa on rakennettu ja arvioitu GDPR:n periaatteita vasten.

Uudistettu ITS-direktiivi (EU/2023/2661) alleviivaa tietosuojaa ja yksityisyyttä koskevia sääntöjä GDPR:n mukaisesti. ITS-direktiivissä määriteltyjä henkilötietoja saa käsitellä siltä osin, kun tarkoituksena on varmistaa tieliikenteen turvallisuus ja turvaaminen sekä tehostettu liikenteen, liikkumisen tai häiriöiden hallinta. Direktiivi edellyttää, että vaikutustenarviointiin on sisällytettävä analyysi vaikutuksesta yksilöiden suojeluun henkilötietojen käsittelyssä. Jos anonymisointi on teknisesti mahdollista, sitä on käytettävä. Jos anonymisointi ei ole teknisesti mahdollista, tiedot ovat pseudonymisoitava mahdollisuuksien mukaan.

Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY, ePrivacy direktiivi): Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annettua Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY sovelletaan henkilötietojen käsittelyyn, joka liittyy yleisesti saatavilla olevien sähköisten viestintäpalveluiden tarjoamiseen yleisissä viestintäverkoissa. Se edellyttää viestinnän ja siihen liittyvien tietoliikennetietojen luottamuksellisuuden varmistamista.

Direktiivin tarkoituksena on yleistä tietosuojasääntelyä täydentäen suojata luonnollisten henkilöiden perusoikeudet ja erityisesti heidän oikeutensa yksityisyyteen, sekä oikeushenkilöiden oikeutetut edut. Direktiivissä sallitaan viestinnän matkaviestinverkoissa vaatimien paikkatietojen käsittely, kun ne ovat välttämättömiä tietoliikennetietoja. Tietoliikennetiedot on poistettava tai tehtävä nimettömiksi, kun niitä ei enää tarvita viestinnän välittämiseen. Muita paikkatietoja kuin tietoliikennetietoja saa käsitellä vain silloin, kun ne on tehty nimettömiksi tai jos käyttäjät tai tilaajat ovat antaneet siihen suostumuksensa. Tietoja saa käsitellä ainoastaan siinä määrin ja niin kauan kuin lisäarvopalveluiden tarjoaminen edellyttää. Matkaviestinverkon mahdollisuus käsitellä tarkempia paikkatietoja ja tarjota lisäarvopalveluita henkilökohtaisten liikennetiedotusten tai opastuksen vuoksi, sallitaan ainoastaan tilaajan suostumuksella.

Direktiivissä säädetään myös tietojen tallentamisesta tai tilaajan tai käyttäjän päätelaitteelle tallennettujen tietojen käyttämisestä. Teleyritysten on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen tarjoamiensa palveluiden turvallisuuden.

European Data Protection Board (EDPB): Euroopan tietosuojaneuvoston tehtävänä on antaa EU:n yleisen tietosuoja-asetuksen (GDPR) ydinkäsitteiden tulkintaa koskevia ohjeita sekä tehdä sitovia päätöksiä rajat ylittäviä käsittelytoimia koskevissa riita-asioissa ja varmistaa siten EU:n sääntöjen yhtenäinen soveltaminen, jotta samaa tapausta ei käsiteltäisi eri tavoin eri oikeudenkäyttöalueilla. EDPB on antanut kannanoton verkottuneiden ajoneuvojen ja liikkuvuuteen liittyvien sovellusten kontekstissa, mutta C-ITS on rajattu tämän ohjeistuksen ulkopuolelle (European Data Protection Board 2021, 11).

Kyberturvallisuutta koskevat säädökset: C-ITS-laitteiden turvallisuuden arviointi ja sertifiointi vaativat kansallisen tai kansainvälisen sertifiointiviranomaisen hyväksynnän.

European AI Act (EAA) on EU-säädös, joka luokittelee tekoälyjärjestelmien riskitasoja ja asettaa niille vaatimuksia. EAA täydentää muita tietosuoja- ja tietoturvakehyksiä (kuten EU:n yleinen tietosuoja-asetus (GDPR)) tarjoamalla AI-spesifisiä suojatoimenpiteitä C-ITS-palveluissa ja verkottuneissa ajoneuvoissa.

Data Governance Act (EU 2022/868): Asetus keskittyy datan hallintaan ja lisää turvallisten datan jakamisen mekanismien luomista, mahdollistaen julkisen ja yksityisen sektorin yhteistyön. Se pyrkii kasvattamaan luottamusta datan käyttöön asettamalla sääntöjä, jotka suojaavat tietojen yksityisyyttä ja turvallisuutta. Tämä voi osaltaan helpottaa C-ITS-palveluiden käyttöönottoa.

Data Act (EU 2023/2854): Tavoitteena on säädellä, kuka voi käyttää ja saada pääsyn dataan EU:ssa. Se pyrkii edistämään kilpailua ja innovointia selventämällä

datan käyttöoikeuksia ja turvaamalla tasapuolisuuden datan arvoketjuissa. Asetus mahdollistaa rekisteröidyt datan välityspalvelut.

8.2.2 Kansalliset vaatimukset

Kansallisen tietosuojan valvonta: Suomessa tietosuojalainsäädännön noudattamista valvoo tietosuojavaltuutettu. Liikenne- ja viestintävirasto Traficomin tehtävänä on valvoa sähköisen viestinnän palveluista annetun lain sekä sen nojalla annettujen säännösten ja päätösten noudattamista. Tietosuojavaltuutettu kuitenkin valvoo mm. sijaintitietojen käsittelyä koskevan lain 20 luvun säännösten noudattamista.

Tietosuojalaki (1050/2018)

Lailla täsmennetään ja täydennetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä annettua Euroopan parlamentin ja neuvoston asetusta EU:n yleinen tietosuoja-asetus (GDPR), ja sen kansallista soveltamista. Laki määrittelee tarkemmin esimerkiksi tietosuojavaltuutetun toimivaltuudet ja menettelytavat Suomessa.

Valvovalla viranomaisella (Tietosuojavaltuutetun toimisto) on tiedonsaanti- ja tarkastusoikeus. Rekisteröidyllä on oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan sitä koskevaa lainsäädäntöä. Valvontaviranomainen voi asettaa uhkasakon edellä kuvattujen määräysten, henkilötietojen käsittelyn rajoittamisen tai tiedonsiirron keskeyttämisen tueksi. (Tietosuojalaki 1050/2018)

C-ITS-kontekstissa tietosuojalaki täydentää henkilötietojen käsittelyn asianmukaiset ja erityiset toimenpiteet sekä tuo tarkentavia teknisiä, menettelyllisiä ja organisatorisia toimenpiteitä rekisteröidyn oikeuksien suojaamiseksi.

Laki sähköisen viestinnän palveluista (917/2014)

Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annettu Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) on pantu kansallisesti täytäntöön pääasiassa sähköisen viestinnän palveluista annetun lain (Laki sähköisen viestinnän palveluista 917/2014) 17 luvun säännöksillä.

Kansallisen lainsäädännön osalta laki sähköisen viestinnän palveluista käsittelee viestinnän luottamuksellisuutta ja yksityisyyden suojaa. Luku 17 tarkentaa sähköisen viestin ja välitystietojen käsittelyä. Välitystiedolla tarkoitetaan oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi sekä tietoa radioaseman tunnisteesta ja radiolähettimen käyttäjästä sekä tietoa radiolähetyksen alkamisajankohdasta, kestosta ja lähetyspaikasta.

Yleisesti vastaanotettavaksi tarkoitettua radioviestintää ja sen välitystietoja saa 136§ mukaisesti käsitellä, jos kyse on esim. hätäkutsusta ja yleisesti vastaanotettavaksi tarkoitettua radioviestinnästä. Muita sähköisiä viestejä ja välitystietoja saa käsitellä viestinnän osapuolen suostumuksella tai jos laissa niin säädetään. Se, joka on ottanut vastaan tai muutoin saanut tiedon sähköisestä viestistä, radioviestinnästä tai välitystiedosta, jota ei ole hänelle tarkoitettu, ei saa ilman viestinnän osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä,

välitystietoa tai tietoa viestin olemassaolosta, ellei laissa toisin säädetä. (Laki sähköisen viestinnän palveluista 917/2014)

Sähköisten viestien ja välitystietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa eikä sillä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Käsittelyn tarkoituksia voivat olla viestinnän välittäminen, viestintäpalveluiden tekninen kehittäminen, tilastollinen analyysi, väärinkäytösten havaitseminen, estäminen ja selvittäminen. (Laki sähköisen viestinnän palveluista 917/2014, 141–143 §).

Sähköisiä viestejä ja välitystietoja on sallittua luovuttaa ainoastaan niille tahoille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Käsittelyn jälkeen sähköiset viestit ja välitystiedot on hävitettävä tai välitystiedot tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, jollei laissa toisin säädetä. Sähköisiä viestejä ja välitystietoja saa käsitellä vain viestinnän välittäjän tai tilaajan lukuun toimiva. (Laki sähköisen viestinnän palveluista 917/2014, 137 §).

Sähköisiä viestejä ja välitystietoja voi käsitellä siinä määrin kuin se on tarpeen viestinnän välittämiseksi ja sovitun palvelun toteuttamiseksi sekä 272 §:ssä säädetyllä tavalla tietoturvasta huolehtimiseksi. (Laki sähköisen viestinnän palveluista 917/2014, 138 §).

Viestinnän välittäjän on tallennettava yksityiskohtaiset tapahtumatiedot luottamuksellisuuden ja yksityisyyden suojan kannalta keskeisiä välitystietoja sisältävissä tietojärjestelmissä tapahtuvasta välitystietojen käsittelystä. Tapahtumatiedot on säilytettävä kaksi vuotta niiden tallentamisesta. (Laki sähköisen viestinnän palveluista 917/2014, 145 §).

Lakia sähköisen viestinnän palveluista voidaan soveltaa C-ITS-palveluissa, jotka ovat laissa mainittuja lisäarvopalveluita (paikantamis- ja tilatietopalvelu). Sijaintitiedoista ja muista liittymän tai päätelaitteen sijainnin ilmaisevien tietojen käsittelystä säädetään lain 20 luvussa. C-ITS-kontekstissa tämä vaikuttaa erityisesti yksityisyyden suojaan pitkän kantaman tiedonsiirtoon perustuvissa viesteissä. Laki määrittelee viestinnän ja välitystietojen käsittelyä koskevat säännökset, jotka kattavat myös matkaviestinverkoissa toteutetut IP-pohjaiset viestit. Viestinnän välittäjillä, kuten teleyrityksillä, on velvollisuus käsitellä välitystietoja laillisesti ja yksityisyyden suojaa turvaten. Välitystietojen käsittelyn tulee olla perusteltua palvelun tarjoamisen kannalta ja niiden säilyttäminen on rajoitettu tiettyihin lakisääteisiin tarkoituksiin. Teleyritys voi käsitellä välitystietoja palvelun tarjoamiseen liittyviin tarpeisiin, mutta tietojen jakaminen kolmansille osapuolille on yleensä kielletty ilman viestinnän osapuolen suostumusta tai muuta laissa säädettyä perustetta. Teleyrityksillä on velvollisuus suojata keräämänsä tiedot ja säilyttää ne ainoastaan tietyn ajan ja vain välttämättömistä syistä.

C-ITS-palvelut saattavat tallentaa ja käyttää ajoneuvojen ja käyttäjien päätelaitteiden tietoja. Palvelun käyttöä kuvaavien tietojen tallentamisesta käyttäjän päätelaitteelle ja näiden tietojen käytöstä säädetään lain 205 §:ssä, jolla pannaan toimeen sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohta. Sen mukaan evästeiden tai muiden palvelun käyttöä kuvaavien tietojen tallentaminen käyttäjän päätelaitteelle ja näiden tietojen käyttö on sallittua palvelun tarjoajalle, jos käyttäjä on antanut siihen suostumuksensa ja palvelun tarjoaja antaa käyttäjälle ymmärrettävät ja kattavat tiedot tallentamisen tai käytön tarkoituksesta. Tämä ei koske tietojen sellaista tallentamista tai käyttöä, jonka ainoana tarkoituksena on

toteuttaa viestin välittämistä viestintäverkoissa tai joka on välttämätöntä palvelun tarjoajalle sellaisen palvelun tarjoamiseksi, jota tilaaja tai palvelun käyttäjä on nimenomaisesti pyytänyt. Tallentaminen ja käyttö on sallittua ainoastaan palvelun vaatimassa laajuudessa ja sillä ei saa rajoittaa yksityisyyden suojaa enempää kuin on välttämätöntä.

Laki yksityisyyden suojasta työelämässä (759/2004) sääntelee työntekijöiden yksityisyyttä koskevia seikkoja työelämässä. Työnantajilla on velvoite kerätä ja säilyttää henkilötietoja työntekijöistään. Työntekijät- ja hakijat puolestaan joutuvat antamaan näitä tietoja työnantajalle. C-ITS-järjestelmän osalta esimerkiksi V2I-viestit todennäköisesti sisältävät henkilötietoja, joten työnantajan tuleen näiden tietojen käsittelyssä noudattaa GDPR:n velvoitteita.

8.2.3 C-ITS-spesifiset vaatimukset yksityisyyden suojalle

C-ITS-asetusehdotus (C/2019/1789) kuvaa EU C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) ja sen liite 4 C-ITS-turvallisuuspolitiikan, jossa määritellään C-ITS-järjestelmien tietoturvallisuuden hallintaa koskevat vaatimukset. Kuten luvussa 3.1 on kuvattu, asetuksen hylkäämisestä huolimatta Euroopan komissio aloitti C-ITS-palveluiden käyttöönoton edistämisen C-ITS-turvallisuus- ja varmennepolitiikan periaatteiden mukaisilla tavoilla. Yksityisyyden suojan määrittelyä on jatkettu yhdessä tietosuojakehityksen kanssa eri organisaatioiden, EU Joint Research Centre (JRC), C-Roads Platform -yhteistyöryhmän ja standardoimisjärjestö ETSI:n, toimesta.

EU Joint Research Centre (JRC) Security Policy

JRC:n laatima politiikkadokumentti (C-ITS Security Policy, 2023*, 4–5)* on päivitetty versio C-ITS-asetusehdotuksen liitteestä 4. Se määrittelee C-ITS-tietoturvapolitiikan Euroopassa ja on tiiviisti sidoksissa EU:n C-ITS-varmennepolitiikan (C-ITS Certificate Policy, 2024) kanssa. Tietoturvapolitiikan tavoitteena on tarjota viitekehys tietoturvan hallinnalle Euroopan C-ITS-järjestelmän käyttöönotossa ja toiminnassa. Se määrittelee, kuinka tietoturvaa hallitaan, ml. tietoturvapolitiikkojen määrittely yksittäisille sidosryhmille ja tietoturvan hallintajärjestelmän toiminta. Tietoturvapolitiikka edellyttää, että C-ITS-yksiköitä operoidaan standardin ISO 27001 tai NIS 2 vaatimusten mukaisesti ja kaikkien C-ITS-yksikköoperaattoreiden on noudatettava tämän dokumentin vaatimuksia.

Dokumentti esittelee luokittelukehyksen tietoturvan ja tietosuojan hallinnalle C-ITS-järjestelmien käyttöönotossa ja toiminnassa. Keskeinen lähestymistapa on varmistaa tiedon *luottamuksellisuus, eheys ja saatavuus*. Raportti korostaa tietojen luokittelua identifioidun riskin mukaan: matala, kohtalainen ja korkea, ja jossa potentiaaliset vaikutukset organisaation toimintaan ja tietoturvatoimenpiteiden prioriteetteihin arvioidaan vastaavasti. Näitä on tarkemmin kuvattu luvussa 4.2.3.

Henkilötietojen suojaus kuuluu luokkaan luottamuksellisuus. Sen osalta tulee arvioida tietojen luvattoman käytön vaikutuksia asteikolla (i) rajoittunut, (ii) vaikea, (iii) vakava tai katastrofaalinen. Lisäksi raportti asettaa käsiteltyjen tietojen osalta vähimmäisvaikutusarvoja, joita C-ITS-sidosryhmien on noudatettava sekä kiinteissä että liikkuvissa C-ITS-yksiköissä. Luokittelu auttaa priorisoimaan tietoturvatoimenpiteitä, mutta silti kaikki viestit on suojattava asianmukaisesti haitallisten seurausten välttämiseksi. (Taulukko 13)

Taulukko 13. C-ITS-viestien vähimmäisvaikutusarvoja tietoturvatoimenpiteiden priorisointiin (C-ITS Security Policy, 2023).

	Kiinteästä C-ITS-yksiköstä peräisin oleva viestiprofiilin tieto	**Liikkuvasta C-ITS-yksiköstä peräisin oleva viestiprofiilin tieto**
Luottamuksellisuus	CAM: matala DENM: matala IVIM: matala MAPEM: matala SPATEM: matala SSEM: matala	CAM: matala DENM: matala SREM: matala Näiden viestiprofiilien sisältämä henkilötieto: kohtalainen
Eheys	CAM: kohtalainen DENM: kohtalainen IVIM: kohtalainen MAPEM: kohtalainen SPATEM: kohtalainen SSEM: kohtalainen	CAM: kohtalainen DENM: kohtalainen SREM: kohtalainen
Saatavuus	CAM: matala DENM: matala IVIM: matala MAPEM: matala SPATEM: matala SSEM: kohtalainen	CAM: matala DENM: matala SREM: kohtalainen

C-Roads Platform

Myös C-Roads Platform -yhteistyöryhmä (C-ITS Security & Governance, 2023) on määritellyt vaatimuksia C-ITS-viestien yksityisyyden suojalle. Keskeisin määrittelyn kohde on C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) ja jo aikaisemmin kuvatun C-ITS-varmennepolitiikan (C-ITS Certificate Policy 2024) sekä erilaisten viestintätekniikoiden, kuten ETSI-turvakuoren ja IP-pohjaisen viestinnän, tarjoama suojaus. Nämä ovat tärkeä osa myös henkilötietojen suojaamista. Yksityisyyden suojaa koskien C-Roads dokumentaatiosta löytyy joitakin tarkennettuja vaatimuksia:

Anonymiteetti: C-ITS-viestejä lähettävät ajoneuvot ja yksiköt käyttävät pseudonyymejä eli ne lähettävät viestejä käyttäen tunnuksia, jotka eivät suoraan paljasta käyttäjän henkilöllisyyttä. Näitä tunnuksia tulee vaihtaa säännöllisesti, jotta mahdollisuus seurata pitkiä aikoja yksittäistä kohdetta vähenee.

Tekninen ja organisatorinen erottelu: C-ITS-varmennepolitiikka määrää tiettyjen roolien teknisestä ja organisatorisesta erottelusta yleisenä suunnitteluperiaatteena. Rekisteröijän (EA, Enrollment Authority) ja valtuuttajan (AA, Authorization Authority) roolit ovat täysin erilliset. Niihin sisältyy pitkän aikavälin avaimiin (todistushakemuksen allekirjoittamiseen) ja lyhytaikaisiin avaimiin (yksittäisten viestien todennukseen) liittyvien prosessien erottelu.

Varmenteen käyttö: Lyhytaikaiset varmenteet, joita käytetään viestien allekirjoittamiseen, muutetaan säännöllisesti C-ITS-yksikössä toimintojen aikana, ja saman varmenteen käytön toistaminen on rajoitettua. Tämän tarkoituksena on vähentää mahdollisuutta jäljittää tai seurata tiettyä käyttäjää pitkällä aikavälillä. C-ITS-varmennepolitiikka määrittää, että enintään 100 varmennetta voi olla aktiivisena kerrallaan viikon voimassaolojakson aikana.

Tietosuoja ja tietojen säilytysaika: Viesteihin sisältyviä henkilökohtaisia tietoja, kuten todistuksia ja tunnisteita, ei tulisi säilyttää pidempään kuin viisi minuuttia, jotta yksityisyys voidaan maksimoida. Tämä lyhyt aikaraja pyrkii estämään henkilökohtaisten tietojen pitkäaikaisen kertymisen ja käytön tutkimattomiin tarkoituksiin ja koskee erityisesti V2I-viestejä.

Todennus ja korotus: Kaikilla viestejä lähettävillä yksiköillä on oltava asianmukainen varmenne varmistaakseen viestien autenttisuuden. Varmenteet ovat lyhytaikaisia ja ne vanhentuvat nopeasti, mikä tarkoittaa, että niiden jatkuva uusiutuminen on tärkeää tietoturvan ylläpitämiseksi.

Viestinnän suojaus: Erilaisten viestintätekniikoiden, kuten broadcast- ja IP-pohjaisten viestien, suojauksen tulee tapahtua standardin ETSI TS 103 097 mukaisesti. Tämä sisältää digitaalisten allekirjoitusten käytön viestien eheyden ja luotettavuuden varmistamiseksi.

C-Roads Security and Governance -dokumentti nostaa esiin, että yksityisyyteen liittyvät ongelmat ovat erilaisia eri asematyyppien välillä. Ajoneuvojen C-ITS-yksiköt, joiden avulla tarjotaan C-ITS-palveluita (yksityisille) loppukäyttäjille, tarvitsevat muuttuvia (pseudonyymejä) allekirjoituksia annettujen vaatimusten mukaisesti. Tämä yksityisyysvaatimus ei välttämättä koske tienvarsiasemia, tieoperaattoreiden ajoneuvoja tai C-ITS-keskusyksiköitä, jotka allekirjoittavat ja lähettävät viestejä niiden puolesta. Lisäksi dokumentti huomauttaa, että tienvarsiyksiköiden viestinnässä tien käyttäjille (I2V) tietosuojaa ei huomioida, koska näissä **I2V-palveluissa henkilötietoja ei käsitellä**. On syytä huomata, että tieoperaattoreiden ja tieliikenneviranomaisten ajoneuvot, joissa on C-ITS-yksiköitä, voivat olla erityisen sääntelyn alaisia. Tämä sääntely koskee erityisesti työntekijöiden valvontaa ja ajoneuvoja käyttävien henkilöiden oikeutta yksityisyyteen. (C-ITS Security & Governance, 2023)

ETSI-standardit

Tietosuojan osalta C-Roads-profiilispesifikaatioissa vaaditaan yhteentoimivuutta erityisesti ETSI standardien (ETSI TS 102 941 V2.2.1, 2022) ja (ETSI TS 103 097 V2.1.1, 2022) kanssa.

ETSI TS 102 941 -dokumentti määrittelee luottamuksen ja yksityisyyden hallinnan vaatimukset älykkäille liikennejärjestelmille (Intelligent Transport Systems, ITS). Tärkeimpiä yksityisyyden suojaa koskevia vaatimuksia ovat PKI-pseudonymiteetin ja erilaisten tunnisteiden linkittämisen ehkäisy. Linkitystä ehkäistään minimoimalla sellaisen tiedon määrä, joka ei muutu tai muuttuu hyvin hitaasti ajan myötä. Jos viestit sisältävät yksityiskohtaista ja muuttumatonta tietoa, kuten ajoneuvon sarjanumero tai erittäin pysyvät tiedot (kuten tietyt laiteasetukset), tällainen tieto voi mahdollistaa näiden viestien linkittämisen samaan ajoneuvoon pitkän aikavälin kuluessa. Linkityksen ehkäisy voidaan toteuttaa käyttämällä tilapäisiä ja usein vaihtuvia tunnisteita sekä näin ehkäistä mahdollisuus yhdistää

saman ajoneuvon lähetykset pidemmän aikavälin kuluessa. Näin ehkäistään esimerkiksi kaksi samanlaista lähetystä eri päivinä.

Dokumentti korostaa myös C-ITS-yksiköiden elinkaaren hallintaa, joka alkaa yksikön valmistuksesta, sisältää rekisteröitymisen ja valtuutuksen ja päättyy elinkaaren loppuun. Sen aikana turvallisuus ja yksityisyys varmistetaan erilaisten teknisten ja organisatoristen toimenpiteiden avulla koko elinkaaren ajan.

ETSI TS 103 097 määrittelee C-ITS-viesteille käytettävän ETSI-turvakuoren, turvakuoreen sisältyvän varmenteiden sisällön ja esitystavan sekä tietoturvaprofiilit CAM- ja DENM-viesteille. Standardi keskittyy turvallisuusotsikoiden ja varmenteiden formaatteihin, mutta ei erityisesti käsittele linkityksen ehkäisyä tai muita yksityisyyden suojaan liittyviä näkökulmia.

8.2.4 Osoitusvelvollisuus ja hallintajärjestelmä ISO/IEC 27701

Tietosuojan osoitusvelvollisuus on keskeinen periaate EU:n yleisessä tietosuoja-asetuksessa (GDPR). Osoitusvelvollisuuden tarkoituksena on näyttää, miten rekisterinpitäjä kunnioittaa rekisteröityjen eli henkilötietojen käsittelyn kohteena olevien tietosuojaa.

Osoitusvelvollisuus voidaan todentaa hyödyntämällä standardien ISO/IEC 27001 ja ISO/IEC 27002 tietosuojalaajennusosaa ISO/IEC 27701, jonka liitteen A (rekisterinpitäjä) hallintakeinojen toteutus vahvistaa GDPR:n velvoitteiden noudattamisen. Liite B kuvaa henkilötietojen käsittelijän velvoitteet. Standardia ISO/IEC 27701 noudattamalla osoitusvelvollisuuden arviointi helpottuu, laatu paranee ja tietosuojalainsäädännön velvollisuudet ovat selkeitä.

Tietosuojan laajennusosa tuo tarkennuksia standardien ISO/IEC 27001 ja ISO/IEC 27002 vaatimuksiin ja hallintakeinoihin. Lisävaatimuksia on tietosuojan osalta organisaation toimintaympäristöön ja suunnitteluun. Hallintakeinojen osalta on ohjeita ja lisätietoja, jotka koskevat hallintakeinojen toteuttamista. Ne tarkentavat tietosuojan osalta kaikkia muita hallintakeinoja paitsi liiketoiminnan jatkuvuuteen liittyviä hallintakeinoja.

Vaatimukset

Organisaation toimintaympäristössä organisaatio määrittelee henkilötiedon käsittelyyn liittyvän roolinsa. Vaatimusten avulla tunnistetaan organisaatiota velvoittava tietosuojalainsäädäntö, viranomaisvaatimukset ja sopimusvaatimukset. Vaatimustenmukaisuus voidaan todentaa henkilötietojen hallintajärjestelmän avulla.

Suunnittelun avulla määritellään tietosuojan arviointi- ja käsittelyprosessi, jolla tunnistetaan henkilötiedon käsittelyyn liittyvät riskit ja varmistetaan, että niitä hallinnoidaan asianmukaisesti. Tietoturvapolitiikka laajennetaan kattamaan tietosuoja ja siinä määriteltyjen tavoitteiden tulee ottaa huomioon tietosuoja.

Tietosuojan hallintakeinot

Tietoturvapolitiikan tulee tukea organisaation toimintaympäristön mukaista roolia ja sisäisten sekä ulkoisten sidosryhmien vaatimustenmukaisuuden täyttymistä. Organisaation tulee nimetä rooli (tietosuojavastaava), johon voi ottaa yhteyttä henkilötiedon käsittelyä koskevissa asioissa, ja osoitettava resurssit, joilla varmistetaan vaatimustenmukaisuuden hallinnan toteutuminen. Tietoturvahäiriöiden

hallintaprosessissa tulee huomioida henkilötiedon tietoturvaloukkauksen tunnistaminen. Prosessissa kuvataan ilmoitusvelvollisuudet: viranomaisilmoitukset, sidosryhmäilmoitukset, ilmoitukset rekisteröidylle sekä henkilötiedon tietoturvaloukkauksen kirjaamisvelvollisuudet.

Organisaation henkilöstön tietoisuutta henkilötiedon käsittelyn vaikutuksista, sisältäen häiriöraportoinnin, tulee pitää yllä. Tietoisuuden kasvattamisen tulee kattaa henkilötiedon tietoturvaloukkauksen tunnistamisen. Henkilötiedon asianmukainen käsittely ja luokittelu on varmistettava, myös alihankintaketjussa. Henkilötiedon käsittelyn sääntöjen noudattaminen tulee varmistaa koko henkilötiedon käsittelyn elinkaaren ajalta. Lisäksi henkilötiedon käsittelyn sääntöjen tulee kattaa lokitietojen käsittely. Sääntöjen noudattaminen varmistetaan salassapitosopimuksin. Henkilötieto tulee tiedonsiirrossa suojata salauksella.

Omaisuudenhallinta ja niiden sisältämä henkilötieto, erityisesti arkaluonteinen henkilötieto, tulee suojata salaamalla. Henkilötiedon käsittelyyn käytetyt laitteet turvataan asianmukaisella suojauksella laitteiden elinkaaren aikana, erityisesti on huomioitava turvallinen hävittäminen fyysisesti.

Henkilötietoa käsittelevien järjestelmien ja palveluiden käytöstä poistettuja tai vanhentuneita käyttäjätunnuksia ei saisi palauttaa käyttäjille pääsyoikeuksien elinkaaren päätyttyä. Henkilötiedon käsittelyyn valtuutettujen käyttäjien toimet tulee pystyä yksilöimään lokienhallinnan avulla. Autentikointi toteutetaan turvallisen todentamisen keinoilla.

Varmuuskopioinnin politiikan tulee huomioida henkilötiedon käsittelyyn ja sen poistamiseen liittyvät lakisääteiset ja sopimukselliset vaatimukset ja rajoitteet. Henkilötietoa sisältävän varmuuskopion tietojen eheys on varmistettava palautuksessa. Palauttamistoimista tulee pitää lokia. Jos varmuuskopioita varastoidaan alihankkijan toimesta, tulee vain valtuutettujen käsitellä niitä, ne tulee suojata salauksella. Näiden suojauskeinojen toteutuminen varmistetaan alihankintasopimuksin.

Lokitietoihin tulee kirjata henkilötietojen käytön yksityiskohtaiset tiedot, kuten lisäykset, muokkaukset ja poistot. Lokitietojen käsittely kattaa alihankkijan henkilötiedon käsittelyn. Lokitiedot tulee olla saatavilla vain valtuutetuille henkilötiedon käsittelijöille, tarvittaessa eriytettynä asiakaskohtaisesti. Lokitietojen hallinnoinnissa tulee huomioida, että henkilötietoja ei saa säilyttää pidempään, kuin on käsittelyn kannalta tarpeellista.

Turvallisen kehittämisen elinkaaren aikana tulee huomioida henkilötiedon suojaamisen vaatimukset ja mahdollisimman vähäinen käsittely. Henkilötietojen käsittelyn riskejä arvioidaan tietosuojan vaikutustenarvioinnin perusteella, ja siten määritellään suojaustarpeet turvallisessa kehittämisessä. Turvallisen kehittämisen elinkaaren lähtökohtaisena tavoitteena on sisäänrakennettu ja oletusarvoinen tietosuoja, myös alihankintaketjussa. Testiaineiston käsittelyssä ei käytetä autenttisia henkilötietoja. Jos sitä ei voida välttää, huomioidaan henkilötietojen asianmukainen suojaaminen. Henkilötiedot tulee hävittää asianmukaisesti, kun niiden käsittely ei ole enää tarpeellista.

Organisaation toimiessa henkilötietojen käsittelijänä sen on toimitettava asiakkaille riippumattomasti tuotettua näyttöä siitä, että tietoturvallisuuden toteutus

tukee tietosuojan toteutumista. Lisäksi voidaan tuottaa teknistä näyttöä sallitun käsittelyn toteutumisesta, myös haavoittuvuustestauksen tuloksien avulla.

Riskienhallinta edellyttää osoitusvelvollisuutta

Kun organisaatio toteuttaa EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisen tietosuojan vaikutustenarvioinnin, organisaatio täyttää osoitusvelvollisuuden riskienhallintaa koskevan osan. Tietosuojalaajennusosa ISO/IEC 27701 antaa konkreettiset työkalut osoitusvelvollisuuden täyttämiseen ja on siten tärkeä menetelmä C-ITS-henkilötietojen rekisterinpitäjälle.

8.2.5 Arvioita yksityisyyden suojan toteutumisesta C-ITS-viesteissä

C-ITS-asetusehdotus (C/2019/1789) hylättiin, mutta sen eteen tehty määrittely ja arviointi muodostavat keskeisen pohjan C-ITS-viestejä ja yksityisyyden suojaa koskevalle arvioinnille. Tässä luvussa perehdytään muutamaan keskeiseen arvioon.

Article 29 Data protection Working Party

Tietosuojatyöryhmä Article 29 oli riippumaton eurooppalainen neuvoa-antava elin, joka käsitteli laajasti tietosuojaan ja henkilötietojen liittyviä asioita. Article 29 -työ on vaikuttanut merkittävästi tapaan, jolla tietosuoja-asiat käsitellään Euroopassa, ja sen perintö elää EU:n yleisen tietosuoja-asetuksen (GDPR) myötä Euroopan tietosuojaneuvoston (EDPB) kautta.

Kannanotossaan "*Processing personal data in the context of C-ITS*" (Article 29 Data Protection Working Party, 2017) Article 29 ottaa kantaa henkilötietojen käsittelyyn C-ITS-viestien yhteydessä. Kannanotto kattaa vain lyhyen kantaman tiedonsiirtoratkaisut, mutta on muuten kattava dokumentti C-ITS-turvatunnusten hallintajärjestelmästä (EU CCMS).

Kannanotossa linjataan selkeästi, että C-ITS-tieto on henkilötietoa ja kerätyn datan minimointiin kiinnitetään huomiota. Tietosuojan kehittämiseksi Article 29 listaa useita edelleen valideja suosituksia:

- Komission tulisi laatia tiekartta EU:n kansalaisten sijaintitietojen lailliselle käsittelylle C-ITS-sovellusten yhteydessä, jossa EU:n laajuisen oikeudellisen instrumentin säätäminen on lopullinen tavoite (GDPR:n artikla 6(1)c).

- Käsittelyperusteen osalta komission tulisi aloittaa EU:n laajuisen oikeudellisen instrumentin säätäminen mahdollisimman pian. Tällaisen oikeudellisen velvoitteen ei pitäisi sallia henkilötietojen yleistä keräämistä ja käsittelyä, vaan oikeudellisen velvoitteen laajuus on arvioitava asianmukaisesti.

- Muita käsittelyperusteita (suostumus, sopimus, oikeutettu etu, yleinen etu) voidaan käyttää vain, jos lausunnossa kullekin niistä tunnistetut kriittiset kysymykset voidaan ratkaista. Yleisen edun osalta edellytetään arviointia, miten kerätty data vaikuttaa rekisteröityihin ja heidän yksityisyysodotuksiinsa, sekä edellytetään lisää suojatoimenpiteitä myös teknisestä näkökulmasta.

- Tietosuojaa koskeva vaikutustenarviointi (GDPR:n artikla 35(10)) tulisi määrätä lainsäädäntöprosessin aikana, jotta riskit ja lieventävät toimenpiteet voidaan selventää alusta lähtien.

- Kaikissa valituissa oikeudellisissa perusteissa ennakkoon asennettujen C-ITS-toimintojen on oletusarvoisesti oltava pois päältä.
- GDPR:n artiklan 25 (Protection by design) säännökset tulee ottaa käyttöön, jotta käyttäjät voivat valita seurantavaihtoehdot (aika, taajuus, sijainnit) oman mieltymyksensä mukaan.
- Turvallisuutta tulisi vahvistaa, jottei C-ITS-tietoa käytetä laittomasti oikeutettujen tarkoitusten ulkopuolella.
- Muita tietosuojan suunnitteluratkaisuja, kuten tietojen yleistämistä tai kohinaa, tulisi ottaa käyttöön, jotta rajoitetaan tarpeetonta altistumista pitkäaikaiseen seurantaan.
- Erityistä huomiota tulisi kiinnittää siihen, kuinka usein varmenteita vaihdetaan, jotta luodaan tasapaino valitun vaihtovälin ja pitkäaikaisen seurannan riskien välillä.
- Rikostuomioihin ja rikkomuksiin liittyviä tietoja ei tulisi lähettää.
- Tiedon laatu tulisi arvioida huolellisesti, jotta vähennetään riskiä väärien hälytysten tuottamisesta tai todellisten hätätilanteiden virheellisestä tulkinnasta.
- Kaikkien C-ITS-alustassa mukana olevien tahojen tulisi selvästi ilmoittaa, miten pitkään ne säilyttävät tietoja, ja kaikkia C-ITS-toimijoita pitäisi kieltää luomasta keskitettyä tietokantaa vaihdetuista viesteistä.

Kannanoton jälkeen on kehitystä tapahtunut. C-Roads-yhteistyöverkoston johdolla on esimerkiksi varmenteiden vaihtamista kehitetty ja määrittelyä täsmennetty. Kerättävän tiedon laadullista arviointia on viety eteenpäin eri foorumeilla, mutta viime kädessä vastuu tiedon luotettavuudesta on C-ITS-viestin allekirjoittajalla. C-ITS-vaatimuksia koskevan delegoidun asetuksen puuttuessa lainsäädäntöä vaativat kohdat ovat edelleen auki.

Euroopan tietosuojaneuvosto (EDPB)

Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB) on riippumaton eurooppalainen elin ja katto-organisaatio, joka kokoaa yhteen Euroopan talousalueen maiden kansalliset tietosuojaviranomaiset sekä Euroopan tietosuojavaltuutetun.

EDBP on ottanut kantaa henkilötietojen käsittelyyn liittyen verkottuneisiin ajoneuvoihin ja liikkumisen sovelluksiin (European Data Protection Board, 2021) EDPB:n näkökulmasta C-ITS-tietosuoja-asiat ovat hyvin erityisiä (mm. ennennäkemättömät määrät paikannustietoja, henkilötietojen jatkuva lähetys, tietojenvaihto ajoneuvojen ja muiden tien infrastruktuurien välillä) ja niiden käsittely edelleen jatkuu Euroopan tasolla, joten C-ITS-henkilötiedot on jätetty EDPB:n kannanoton ulkopuolelle. C-ITS:n osalta EDPB viittaa edeltäjänsä eli tietosuojatyöryhmä Article 29 kannanottoon. EDPB:n kannanotosta saa kuitenkin hieman tuoreemman käsityksen sen suhtautumisesta C-ITS:n kaltaisiin käyttötapauksiin ja dataan. Lisäksi tietosuojan käsittelyä autojen hätäviestijärjestelmä eCallin osalta voinee pitää eräänlaisena ennakkotapauksena.

EDPB korostaa, että paikkatiedon käyttö vaatii erityisiä suojaustoimenpiteitä, jotta yksilöiden valvonta ja datan väärinkäyttö voidaan ehkäistä. Tiedot voivat

paljastaa työpaikan ja asuinpaikan lisäksi myös kuljettajan kiinnostuksen kohteet vapaa-aikana sekä mahdollisesti arkaluonteista tietoa esim. uskonnon harjoittamisesta tai seksuaalisesta suuntautumisesta vieraillun paikan perusteella.

Lisäksi kannanotossa korostetaan, että ajoneuvojen kuljettajat ja matkustajat eivät välttämättä saa riittävästi tietoa ajoneuvossa tai sen kautta tapahtuvasta tietojen käsittelystä. Tieto saatetaan antaa vain ajoneuvon omistajalle, joka ei välttämättä ole kuljettaja. Myös ajoneuvon omistus saattaa vaihtua joko myynnin tai vuokrauksen vuoksi. EDPB painottaa, että tietojenkäsittelyn perustuessa suostumukseen, kaikki pätevän suostumuksen elementit on täytettävä. Tämä tarkoittaa, että suostumuksen tulee olla vapaa, tarkka ja annettu tietoisen valinnan perusteella, ja sen tulee tarkoittaa rekisteröidyn selkeää tahtoa.

Rekisterinpitäjien tulee kiinnittää erityistä huomiota erilaisten osallistujien, kuten auton omistajien tai käyttäjien, pätevän suostumuksen hankkimisen menettelytapoihin. Sähköisen viestinnän tietosuojadirektiivin mukaan suostumus tulee saada käyttäjältä tai tilaajalta. Suostumus on annettava erikseen erityisiä tarkoituksia varten, eikä sitä saa sitoa uuden auton ostoon tai vuokraamiseen liittyvään sopimukseen. Suostumus on voitava peruuttaa yhtä helposti kuin se on annettu. C-ITS-viestien yhteydessä tämä asettaa suuria haasteita hyödyntää käsittelyperusteena suostumusta.

Suostumusvaatimusta sovelletaan ePrivacy-direktiivin artiklan 5(3) (sekä GDPR:n mukaisesti) tiedon tallentamisessa tai pääsyssä jo tallennettuun tietoon liitettyjen ajoneuvojen yhteydessä. Tämä vaatimus voidaan poistaa kahdessa erityisessä tilanteessa. Jos tiedon tallentaminen tai pääsy tietoihin on tarpeen pelkästään viestinnän välittämiseksi sähköisessä viestintäverkossa, suostumus ei ole tarpeen. Suostumusta ei myöskään tarvita, kun tiedon tallentaminen tai pääsy tietoihin on välttämätöntä käyttäjän tai tilaajan nimenomaisesti pyytämän tietoyhteiskunnan palvelun tarjoamiseksi. Tämä tarkoittaa, että jos käyttäjä on esimerkiksi pyytänyt GPS-navigointipalveluita, jotka vaativat pääsyä laitteen sisäiseen tietoon, suostumus ei ole pakollista.

Lainvalvontaviranomaiset voivat vaatia käsittelyä verkkoon liitettyjen ajoneuvojen keräämistä tiedoista. Tässä tapauksessa tällaisten tietojen katsotaan liittyvän rikostuomioihin ja rikkomuksiin GDPR:n 10 artiklassa ja muussa sovellettavassa kansallisessa lainsäädännössä säädetyin edellytyksin. Euroopan tietosuojaneuvosto huomauttaa, että henkilötietojen käsittely yksinomaan lainvalvontaviranomaisten esittämien pyyntöjen täyttämiseksi ei ole GDPR:n 5 artiklan 1 kohdan b alakohdassa tarkoitettu tietty, nimenomainen ja laillinen tarkoitus.

Kun sähköisen viestinnän tietosuojadirektiivi ei edellytä rekisteröidyn suostumusta, rekisterinpitäjän vastuulla on kuitenkin valita GDPR:n 6 artiklan mukainen oikeusperuste, joka soveltuu parhaiten henkilötietojen käsittelyyn (European Data Protection Board, 2021, 14).

Kansallisten tieviranomaisten TIARA-projekti

TIARA-projekti (Trusted Integrity and Authenticity for Road Applications) tarjoaa kansallisille tienviranomaisille (National Road Authority, NRA) laajemman näkemyksen ja tietoa siitä, mitä vaaditaan luotettavan ja turvallisen tietoinfrastruktuurin saavuttamiseksi. Luonnosvaiheessa olevalla raportilla (Maerivoet & Ons 2023) halutaan varmistaa, että tienkäyttäjät voivat luottaa tienpitäjien käsittelevän C-

ITS-tietoa laillisin ja tarkoituksenmukaisin keinoin. Raportti auttaa tienpitäjiä ymmärtämään käsittelemänsä tienkäyttäjien sijaintitiedon vaikutukset yksityisyyden suojaan sekä antaa suosituksia tämän tiedon käsittelyyn.

Dokumentissa tunnistetaan useita rekisteröidystä kerättäviä henkilötietoja, kuten sijaintitiedot, biometriset tiedot, ajoneuvon tekniset tiedot, ajokäyttäytymistiedot sekä info- ja viihdejärjestelmien sisältämät tiedot.

Raportin lähtökohtana on, että C-ITS-viestit ovat henkilötietoa. Henkilötietoa niistä tekee erityisesti PKI-varmenteen käyttäminen sekä viestien otsikkokentän tiedot, aikaleimat ja mahdolliset tarkasteltavan ajoneuvon mittatiedot. Kirjoittajat nostavat esille kokemukset Belgiassa toteutetusta ViaPass-projektista, jossa tietoa on systemaattisesti kerätty raskaiden ajoneuvojen pseudonymisointia käyttävistä ajoneuvoyksiköistä. Projektissa on osoitettu, miten ajoneuvojen jäljitys saadaan tästä huolimatta toteutettua jopa minimaalisella määrällä sijaintipisteitä (Maerivoet & Ons 2023, 18). Raportissa on tarkasteltu yksityisyyden suojaa koskevia tutkimusraportteja myös C-ITS-kontekstin ulkopuolelta, joten suoria johtopäätöksiä tulee välttää.

Raportissa korostetaan, että Euroopassa käytettävien ajoneuvojen tietosuoja määräytyy pääasiassa EU:n yleisen tietosuoja-asetuksen (GDPR) mukaan. GDPR:n ja Euroopan tietosuojaneuvoston (EDPB) ohjeiden mukaisesti rekisteröidyille annetaan oikeus tarkastaa, oikaista ja poistaa heitä koskevia tietoja. Tämä varmistaa, että käyttäjillä on merkittävä kontrolli heidän henkilötietojensa käsittelyssä. Sisäänrakennettu tietosuoja on keskeisessä roolissa verkottuneiden ajoneuvojen ekosysteemien rakentamisessa. Ohjeissa korostetaan, että kerättävien ja käsiteltävien tietojen minimointi on tärkeää ja että tietojen käsittelystä on kommunikoitava avoimesti rekisteröidyille. Monet autovalmistajat pitävät tiukkaa sääntelyä hyvänä, koska sen uskotaan varmistavan kuluttajien luottamusta, mikä on olennaista C-ITS:n laajamittaisessa hyödyntämisessä (Maerivoet & Ons 2023, 43–46).

Raportissa arvioidaan mahdollisuuksia, jotka liittyvät yksittäisen ajoneuvon tunnistamiseen sekä sijaintitiedon anonymisoinnin murtamiseen eli deanonymisointiin. Riskien lieventämiseksi tarjotaan yleiskuva toimenpiteistä ja menetelmistä, joita käytetään riskien vähentämiseksi, sekä arvioidaan lisätoimenpiteiden tarvetta. Lisätoimenpiteet riskienhallintaan ovat teknologisia, sääntelyyn perustuvia ja organisatorisia keinoja tietosuojan ja yksityisyyden suojaamiseksi ajoneuvodatan käsittelyssä. Keinoina esitetään mm. anonymisoinnin, uusien kryptografisten menetelmien ja tiedon määrän minimoinnin yhdistelmää, tiedonvaihdon keskeyttämistä kriittisissä kohteissa kuten kodeissa ja työpaikoilla sekä lohkoketjuteknologian hyödyntämistä. C-Roads-määrittelyt eivät näitä keinoja vielä tunne.

Vaikutustenarvioinnin keskeinen tarkoitus on arvioida, mitä tietoa C-ITS-viestit voivat paljastaa tienkäyttäjistä ja mikä on tällaisten tietojen paljastumisen mahdollinen vaikutus yksilöihin. C-ITS-tiedon tuottamat hyödyt muun muassa liikenneturvallisuudelle ovat huomattavia, mutta ne sisältävät myös merkittäviä yksityisyysriskejä. Tarkastelussa on erityisesti ajoneuvodatan, kuten sijainnin, nopeuden ja suuntatiedon, korrelointi henkilökohtaisten tietojen kanssa. Näitä tarkastellaan yksityiskohtaisemmin luvussa 8.5.1. Kehittyneiden analysointitekniikoiden myötä mahdollisuus henkilön tunnistamiseen pseudonymisoidusta aineistosta kasvaa, mikä tekee nykyisten ja tulevien tietosuojatoimenpiteiden jatkuvan kehittämisen välttämättömäksi. Vaikutustenarviointi on tarpeellista, jotta ymmärretään, miten

erilaisten tietojen yhdistely ja analysointi voivat vaikuttaa yksilöiden yksityisyyteen.

Kokonaisuudessaan dokumentissa tunnustetaan rekisteröidyn oikeuksien merkitys GDPR:n mukaisessa henkilötietojen käsittelyssä, ja vaaditaan, että tietojen käsittelijöiden tulee noudattaa näitä sääntöjä ja suojatoimia tietojen suojaamiseksi ja rekisteröidyn oikeuksien toteuttamiseksi. Olemassa olevan regulaation rooliksi nähdään määritellä enemmän lopputulema ja periaatteet. Jäsenvaltioiden ja alan toimijoiden tulee itse määrittää parhaat tekniset toimenpiteet näiden vaatimusten täyttämiseksi. (Maerivoet & Ons 2023, 59).

8.2.6 Ennakkotapauksena eCall

Autojen hätäviestijärjestelmä eCall on ollut pakollinen ajoneuvoluokkien M1 ja N1 (henkilö- ja pakettiautot) uusissa ajoneuvomalleissa jo vuodesta 2018 saakka. eCall-ajoneuvolaite lähettää hätäkeskukselle eCall-järjestelmän minimitietopakettiin (MSD, minimum set of data) ja avaa puheyhteyden ajoneuvossa olevien ja hätäkeskuksen välille. eCall-järjestelmän minimitietopakettiin sisältyy mm. tiedot onnettomuuden sijainnista ja ajankohdasta, ajoneuvon VIN-numero, ajoneuvoluokka sekä ajoneuvon käyttövoima.

Euroopan tietosuojavaltuutettu (EDPS) on kannanotossaan nostanut yksityisyyden suojan toteutumisen eCall-järjestelmässä yhdeksi esimerkiksi (European Data Protection Board, 2021, 30), joten C-ITS-toteutusta koskevan kannanoton puuttuessa se muodostanee hyvän ennakkotapauksen.

Henkilötietojen käsittelyä koskevan sääntelyn yleisenä viitekehyksenä on GDPR. Lisäksi sähköisen viestinnän tietosuojadirektiivi (EU 2002/58, 2002, ePrivacy) asettaa säännöstön toimijoille, jotka haluavat tallentaa tai käyttää tilaajan tai käyttäjän päätelaitteelle tallennettuja tietoja Euroopan talousalueella (ETA). Tärkeänä lähtökohtana on, että eCall-järjestelmää käsittelevä asetus (EU) 2015/758 syrjäyttää tarpeen kuljettajan suostumukselle sijaintitietojen ja eCall-järjestelmän minimitietopaketissa (MSD, minimum set of data) välitettävien henkilötietojen käsittelyssä sekä muodostaa GDPR:n mukaisen oikeudellisen velvollisuuden tietojen käsittelylle. (European Data Protection Board 2021, 31).

eCall-järjestelmän toimintaa käsittelevässä asetuksessa (EU) 2015/758 todetaan, ettei asetuksen mukaisesti käsiteltyjä tietoja tule säilyttää pidempään kuin hätätilanteiden käsittely edellyttää. eCall-ajoneuvolaitteen sisäiseen muistiin tallennettavia tietoja on myös poistettava säännöllisesti ja jatkuvasti. Vain ajoneuvon kolme viimeisintä sijaintia voidaan tallentaa ajoneuvon suunnan määrittämiseksi ja MSD-viestin muodostamiseksi. Delegoitua asetusta (EU) 2015/758 on sittemmin muutettu kaksi kertaa. Edellä mainitut kohdat ovat kuitenkin mukana myös asetuksen nykyisessä versiossa.

Rekisteröidyn oikeudet ja rekisteröidyn informointi

Ajoneuvojen kuljettajat ja matkustajat eivät välttämättä aina saa riittävästi tietoa verkkoon liitetyssä ajoneuvossa tai sen välityksellä tapahtuvasta tietojen käsittelystä. Tiedot saatetaan antaa ainoastaan ajoneuvon omistajalle, joka ei välttämättä ole auton kuljettaja. Ajoneuvon elinkaaren aikana sillä voi olla useita omistaja, jolloin rekisteröidyn informointia ei voida välttämättä varmistaa.

eCall-järjestelmää koskevassa asetuksessa (EU) 2015/758 edellytetään, että valmistaja toimittaa ajoneuvon käyttöohjeen yhteydessä selkeät ja täydelliset tiedot, miten eCall-ajoneuvolaite käsittelee henkilötietoja. Tämä tieto on annettava käyttöohjekirjassa erikseen 112-pohjaista eCall-ajoneuvojärjestelmää ja kaikkia kolmannen osapuolen palvelun tukemia eCall-järjestelmiä varten ennen järjestelmän käyttöä. Käyttäjää on muistutettava, mitä tietoja kerätään, ja järjestelmän olevan oletusarvoisesti aina aktiivisessa tilassa. Käyttäjää on myös informoitava, ettei ajoneuvoa seurata jatkuvasti, vaan tietoa jaetaan vain hätätilanteessa.

Käyttäjää on myös informoitava rekisteröityjen oikeuksista. On huomattava, että käsittely perustuu oikeudelliseen velvoitteeseen, joten oikeus vastustaa ja oikeus tietojen siirrettävyyteen eivät ole sovellettavissa eCall-järjestelmän yhteydessä. (European Data Protection Board 2021, 32).

eCall-viestien vastaanotto ja turvallisuus

eCall-ajoneuvolaitteen tietoja ei saa jakaa ajoneuvolaitteen ulkopuolelle, ennen kuin ajoneuvolaite aktivoidaan. Välittömästi aktivoinnin jälkeen eCall-ajoneuvolaite muodostaa puheyhteyden ajoneuvossa olevien ja hätäkeskuksen välille sekä lähettää eCall-järjestelmän minimitietopaketin (MSD, minimum set of data) hätäkeskukseen. Ajoneuvossa oleva käyttäjä voi aktivoida eCall-ajoneuvolaitteen manuaalisesti. Aktivointi voi tapahtua myös automaattisesti ajoneuvossa olevien sensoreiden havaittua onnettomuuden.

112-pohjaisen eCall-hätäviestipalvelun kautta lähetetyt ja hätäkeskuksen käsittelemät tiedot voidaan siirtää muille viranomaisille ja muille määritellyille palvelukumppaneille vain hätätapauksissa ja asetettuja ehtoja noudattaen. Hätäkeskuksen 112-pohjaisen eCall-hätäviestipalvelun käsittelemiä tietoja ei siirretä muille kolmansille osapuolille ilman rekisteröidyn nimenomaista etukäteissuostumusta.

eCall-järjestelmää koskeva delegoitu asetus (EU) 2015/758 määrittelee vaatimukset eCall-hätäviestipalveluun sisällytettäville teknologioille, jotka vahvistavat yksityisyyden suojaa. Tätä pidetään välttämättömänä, jotta käyttäjille voidaan tarjota asianmukainen yksityisyyden suoja sekä tarvittavat takeet valvonnan ja väärinkäytösten estämiseksi. Lisäksi valmistajien tulisi varmistaa, että 112-pohjainen eCall-hätäviestipalvellun, samoin kuin kaikki muut kolmannen osapuolen palveluiden tai lisäarvopalveluiden tarjoamat eCall-järjestelmät, on suunniteltu siten, että henkilötietojen vaihtaminen näiden järjestelmien välillä on mahdotonta.

Hätäkeskusten osalta jäsenvaltioiden tulisi varmistaa, että henkilötiedot suojataan väärinkäytöltä, mukaan lukien laiton pääsy, muuttaminen tai menetys. Lisäksi on tärkeää, että henkilötietojen tallennusta, säilytysaikaa, käsittelyä ja suojaa koskevat protokollat ovat asianmukaisella tasolla ja että niitä noudatetaan tarkasti.

8.2.7 Johtopäätökset vaatimuksista

C-ITS-asetusehdotuksen kohtalosta huolimatta kehitystä on jatkettu, ja esimerkiksi EU:n C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) osalta on saatu paljon konkreettista aikaiseksi. EU:n tasolla datan hallintaa ja tietosuojaa on viime vuosina kehitetty laaja-alaisesti, mutta C-ITS-viestien erityiskysymysten osalta lainsäädäntö on edelleen puutteellista. Merkittävimpänä puutteena voidaan pitää selkeän käsittelyperusteen puuttumista. C-ITS-viestien osalta tätä on haastava ratkaista yksiselitteisesti muuten kuin säätämällä käsittelyperusteeksi

lakisääteinen velvollisuus tai vähintään määrittelemällä lainsäädännöllinen peruste, joka avaa mahdollisuuden hyödyntää käsittelyperusteena yleistä etua. eCall-hätäviestipalvelun osalta asia on ratkaistu säätämällä lakisääteinen velvollisuus. Vaatimusten ristiriitaisuutta kuvastaa, että ajoneuvovalmistajat keräävät laajasti tietoa myymistään ajoneuvoista ja niiden omistajista käsittelyperusteenaan oikeutettu etu.

Tietosuojatyöryhmä Article 29 on jo vuonna 2017 nostanut esiin myös muita puutteita C-ITS-järjestelmän yksityisyyden suojassa. Tietosuojaa koskeva vaikutustenarviointi tulisi määrätä lainsäädäntöprosessin aikana, jotta riskit ja lieventävät toimenpiteet voidaan selventää alusta lähtien. Lisäksi kannanotossa kaivataan lainsäädäntöä sijaintitietojen lailliselle käsittelylle C-ITS-sovellusten yhteydessä. Mukana on myös useita vaatimuksia koskien datan laatua, ajoneuvon jäljittämisen vaikeuttamista teknisin keinoin sekä datan viestikohtaisia säilytysaikoja.

Yksityisyyden suojan osalta C-ITS-viestien käyttöönottoa vaikeuttaa määrittelyiden puuttuminen erityisesti C-Roads-profiilispesifikaatioissa määritellyn pitkän kantaman tiedonsiirtoratkaisun sekä hybridiympäristöjen osalta. C-Roads-profiilispesifikaatiot ovat niiden osalta vielä puutteelliset. Koko luottamusmalli ei edes kata pitkän kantaman tiedonsiirrossa viestien kannalta keskeistä osuutta eli niiden välittämistä matkaviestinverkolla C-ITS-keskusyksikön ja ajoneuvon välillä. Tältä osin henkilötiedon muodostuminen riippuu valitusta mobiiliteknologiasta.

Pseudonymisointi on pitkälle kehitetty, joten moniin varmenteiden voimassaoloa ja vaihtoa koskeviin vaatimuksiin on kyetty vastaamaan. Riskien hallinnan kannalta esim. maksimissaan 5 minuutin säilytysaika henkilötietoa sisältäville V2I-viesteille hankaloittaa käyttäjän seuraamista. Pseudonymisointi ei kuitenkaan takaa datan anonymiteettiä ja tiedon yhdisteltävyys avaa lähes loputtomat mahdollisuudet henkilötiedon muodostumiseen. Vaatimuksen jatkuvaan parantamiseen riskien hallinnan ja hallintajärjestelmän menetelmien mukaan ovat tarpeen.

C-ITS-viestit kattava delegoitu asetus tulisi tarpeeseen. Epäselvyys jo vanhojen virallisten kannanottojen, esille nostettujen ongelmien ja tehtyjen parannusten välillä luo epävarmuutta kykyyn toteuttaa GDPR:n mukaista tietosuojaa. Lisää epäselvyyttä alalle luo esimerkiksi autonvalmistajien laajat käytännöt kerätä dataa ajoneuvoista, SRTI- ja RTTI-asetusten mukainen eteneminen ja useissa maissa etenevät C-ITS-investoinnit. Kannanotoissa on nostettu esille perustavanlaatuisia sijaintitietoon, käsittelyperusteeseen ja rekisteröidyn oikeuksiin liittyviä ongelmia. Esimerkiksi autovalmistajat keräävät laajasti autoon liittyvää henkilötietoa vedoten oikeutettuun etuun, vaikka kannanotot puhuvat kuljettajan laadukkaan suostumuksen puolesta.

8.3 C-ITS-viestien sisältämä henkilötieto

C-ITS-palvelut koostuvat laajasta joukosta erilaisia käyttötapauksia, ja niissä välitetään erilaista informaatiota. Palveluiden tiedonsiirtoa varten on määritelty C-ITS-viestiprofiileita. Viestiprofiileita tutkimalla voidaan selvittää, liikkuuko niissä henkilötietoa. Tässä luvussa tarkastellaan, mitä tietosisältöä eri C-Roads-profiilispesifikaation mukaisissa C-ITS-viestiprofiileissa välitetään, ja onko sisältö mahdollisesti henkilötietoa.

Luvussa 6.2.2 on kuvattu C-ITS-viestien tyypillinen rakenne. Viestirakenteen keskeiset osat ovat

- **ETSI-turvakuori**, jonka sisällä välitetään allekirjoitetun C-ITS-viestin varsinainen informaatiosisältö (payload).
- **Lyhyen kantaman tiedonsiirron C-ITS-viesti.** Viesti koostuu GeoNet Basic Header -otsikosta sekä sisältää tietoa viestin perusreititystä ja käsittelyä varten. C-ITS-viestien sisältö on pelkästään allekirjoitettu. Allekirjoitus varmistaa viestin eheyden ja muuttumattomuuden, mutta ei salaa viestin sisältöä.
- **TLS-turvakuori pitkän kantaman tiedonsiirrossa**. TLS-protokolla muodostaa IP-pohjaisessa pitkän kantaman tiedonsiirrossa turvallisuutta suojaavan kuoren lyhyen kantaman tiedonsiirrossa käytettävälle viestille. Se tarjoaa viestintään salauksen, viestien eheyden tarkistuksen ja autentikoinnin.

8.3.1 GDPR:n mukainen henkilötieto C-ITS-viesteissä

EU:n yleisen tietosuoja-asetuksen (GDPR) mukaan henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

GDPR luokittelee myös profiloinnin henkilötiedoksi, koska profilointi perustuu henkilötietojen käyttöön. Profilointi tarkoittaa mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin.

C-ITS-viesteissä henkilötietoa arvioidaan syntyvän esimerkiksi seuraavasti (Maerivoet & Ons 2023, 66):

Ajoneuvon ominaisuudet ja tilat: sijainti ja liikkumistiedot (koordinaatit nopeudet, suunta, kiihdytykset, hidastukset, jne.) voivat paljastaa kodin tai työpaikan sijainnin. Ne saattavat kertoa päivittäisistä rutiineista, käytetyistä reiteistä sekä lähtö- ja saapumisajoista. Ajotapa saattaa olla sormenjäljen tai kävelytavan kaltainen yksilöllinen tunniste. Se voi kertoa myös henkilön riskisietoisuudesta tai aggressiivisesta ajotavasta, jotka saattavat kiinnostaa viranomaisia tai vakuutusyhtiöitä. Ajoneuvon koko ja tyyppi saattavat kertovat henkilökohtaisista valinnoista, taloudellisesta tilanteesta ja elämäntyylistä.

Ajoneuvo- ja laitetunnisteet: saattavat mahdollistaa tilapäisten ID-tunnisteiden linkittämisen pysyviin tunnisteisiin kuten rekisterinumeroon ja sitä kautta omistajan henkilötietoihin. Useiden ajoneuvojen liikkuminen toistuvasti yhdessä saattaa viestiä henkilöiden välisistä suhteista.

Aikatiedot: viestin generointiajat saattavat korreloida henkilökohtaisten aikataulujen kanssa ja siten paljastaa työaikoja, vapaa-ajan aktiviteettejä, osallistumista tapahtumiin tai sosiaalisiin kokoontumisiin.

Risteysten ja tieväylien tiedot: kertovat käytetyistä teistä ja kaistoista ja saattavat siten muodostaa lähes sijaintitiedon kaltaista tietoa ajoneuvon liikkeistä.

Näiden lisäksi on syytä huomioida, että henkilötieto on määritelmällisesti henkilöön yhdistettävissä olevaa tietoa ja yhdistäminen saattaa tapahtua myös lisätietoja käyttäen. Tällaista lisätietoa on saatavilla mm. ajoneuvovalmistajilla tai teleoperaattoreilla. Eräänlainen äärimmäinen esimerkki henkilötiedon syntymisestä voisi olla seuraava. Ajoneuvon mobiililiittymällä jaetaan WiFiä, jonka kautta jaetaan tekijänoikeuden suojaamaa materiaalia. Tekijänoikeuksien haltijoiden edustajilla on oikeus saada tuomioistuimen kautta ko. ajankohdan IP-osoitteen käyttäjän tiedot Internet-palveluntarjoajalta, jolloin IP-osoite yhdistyy orastavaan oikeudellisen prosessin kautta vastaajan henkilötunnukseen. Esimerkki korostaa pseudonymisoinnin puutteita riskinhallintakeinona. Vain anonymisointi eli henkilötiedon poistaminen on keino vapautua GDPR-vaatimuksista ja se on käytännössä vaikeaa.

Henkilötietojen määritelmää on syytä arvioida myös siitä näkökulmasta, kenelle sama tieto on henkilötietoa ja kenelle ei. EU:n delegoitu asetus tieliikenteen turvallisuustiedoista eli SRTI-asetus (EU) 2013/886 tarjoaa tästä hyvän esimerkin. SRTI-asetuksen mukaiset tietolajit ovat ajoneuvoista kerättäviä V2I-tietoja ja sisältävät henkilötietoja. Tietojen keräämisen tyypillisesti suorittavat autonvalmistajat, jotka ovat rekisterinpitäjiä ja kuvaavat henkilötietojen käsittelyn tietosuojaselosteessa. SRTI-asetuksen mukaan näitä tietoja on kerättävä myös kansalliseen yhteyspisteeseen (NAP). Tämä toteutetaan yhteisen EU:n yhteistyöelimen Data for Road Safety (DfRS) määrittelemin keinoin. DfRS kertoo tietosuojaselosteessaan (Data for Road Safety, 2021), että sopimuksensa mukaan he saavat autonvalmistajilta vain anonymisoitua tietoa ajoneuvoista, ja yksittäisen ajoneuvon tietoja siitä ei voida jäljittää. Näillä ollen DfRS hyödyntää vain anonymisoitua dataa eikä käsittele henkilötietoja.

8.3.2 Eri C-ITS-viestien sisältämä henkilötieto (Payload)

Edellä esitetyn perusteella voidaan arvioida erityyppisiin C-ITS-viesteihin sisältyviä henkilötietoja. C-ITS-viestiprofiilin mukainen tietosisältö kulkee allekirjoitettuna ETSI-turvakuoren sisällä. Tämä tietosisältö on yhteinen lyhyen ja pitkän kantaman tiedonsiirrossa käytettäville viesteille. Alla olevassa taulukossa 14 esitetään eri C-ITS-viestityyppien (C-Roads C-ITS Message Profiles 2023) tietosisältö, johon mahdollisesti voi sisältyä henkilötietoja.

Taulukko 14. Eri C-ITS-viestityyppien sisältämä potentiaalinen henkilötieto.

C-ITS-viestiprofiili	Esimerkkejä tietosisällöstä, joka saattaa sisältää henkilötietoa
DENM: Decentralized Environmental Notification Message	DENM-viestiprofiilissa välitetään Hazardous Location Notification (HLN) ja Road Works Warning (RWW) viestejä, joilla varoitetaan esimerkiksi vaaraa aiheuttavista tapahtumista tai kunnossapitotöistä tieverkolla. Viestit ovat tyypillisesti I2V-viestejä, joten henkilötietoa näissä viesteissä ei synny. Henkilötietoa saattavat luoda esim. kunnossapitotöissä olevat tieoperaattorin ajoneuvot (V2I). **actionID**: viestin yksilöivä tunniste sisältää tiedon C-ITS-yksiköstä (esimerkiksi tietyövaunun tunnistenumero), joka on muodostanut viestin. **detectionTime, referenceTime:** havainnon tarkka aika. **eventPosition, lanePosition**: tiellä olevan esteen, tapahtuman tai olosuhteen tarkka paikkatieto (pituus-, leveys- ja korkeuskoordinaatit). **eventSpeed**: kohteen liikenopeus. **stationType**: kertoo C-ITS-yksikön tyypin (esimerkiksi tienvarsiyksikkö, kiinteä tai siirrettävä) tai ajoneuvon tapauksessa rekisteröinnin mukaisen ajoneuvotyypin. **traces**: kertoo reittipisteet, joiden kautta kohdetta tai tapahtumaa lähestytään. Tukee erityisesti automaattiajamista toteuttamaan turvallisia valintoja.
IVIM: In-Vehicle Information Message	IVIM-viestiprofiilissa välitetään In-Vehicle Signage ja Automated Vehicle Guidance viestejä. Viesteillä voidaan esimerkiksi informoida kuljettajia liikennemerkeistä tai edesauttaa automaattisia ajoneuvoja toteuttamaan tienpitäjän suosimia päätöksiä. Viestit ovat tyypillisesti I2V-viestejä eivätkä sisällä henkilötietoja. **timestamp**: viestin muodostamisen ajankohta . **referencePosition, zone**: paikka- ja aluetieto. **RoadConfiguration, roadType, laneConfiguration, LaneInformation**: kertovat tarkat tiedot alueella olevista kaistoista. **code**: ISO 14823 -standardin mukainen liikennemerkin koodi. **TextContainer**: kaikki liikennemerkkiin liittyvä vapaa tekstitieto. **direction**: liikennemerkin vaikutussuunta. **allowedSaeAutomationLevels**: sallitut SAE-automaatiotasot. **PlatooningRule**: tietoja letka-ajon sallimisesta, letka-ajoon osallistuvien ajoneuvojen lukumäärä, nopeus, välimatkat ja letkan pituus.

C-ITS-viestiprofiili	Esimerkkejä tietosisällöstä, joka saattaa sisältää henkilötietoa
SPATEM, MAPEM:	MAPEM-profiilissa välitetään risteyksen tunniste ja tarkkaa paikkatietoa, kuten risteyksen topologiasta ja kaistatiedoista. SPATEM-viesteissä välitetään liikennevalojen tilatieto. Viestit ovat tyypillisesti I2V-viestejä. **IntersectionGeometry and RoadSegment**: määrittelevät tarkan risteysgeometrian (kaistojen lukumäärä, liikennevalojen paikka, suojatiet, jne.) ja tiesegmentit risteysalueiden ulkopuolella. Nämä tiedot voidaan linkittää esimerkiksi ajoneuvojen CAM-viestien tuottaman reaaliaikaisen datan kanssa. **RegulatorySpeedLimit and AdvisorySpeed**: määrittelevät nopeusrajoituksen ja suositusnopeuden risteystä lähestyttäessä. **GenericLane and NodeXY**: kaistatason geometriset ja toiminnalliset yksityiskohdat risteyksissä sekä solmukohdat eli pisteet kaistageometriassa, jotka tarjoavat lisää kontekstia liikennejärjestelyille risteyksissä tai muissa kriittisissä pisteissä. **IntersectionState**: risteyksen liikennevalojen tilatietoa ja tietoa ajoituksista. **MovementState**: yksityiskohtaisempaa tietoa liikennevalojen yksittäisen signaaliryhmän ajoituksista ja suositellusta lähestymisnopeudesta.
SREM, SSEM SREM (Signal Request Extended Message) SSEM (Signal Status Extended Message)	SREM- ja SSEM-viestiprofiileita käytetään joukkoliikenteen ja hälytysajoneuvojen priorisointiin liikennevalo-ohjatuissa risteyksissä. Viestit ovat tyypillisesti V2I-viestejä. **requestor**: voivat sisältää tunnisteita signaalien prioriteettia tai etuutta pyytävästä tahosta (esim. hätäajoneuvo, julkinen liikenne). **SignalRequestPackage**: sisältää tietoja pyydetystä liikkumisesta risteyksissä. Tätä voidaan hyödyntää esimerkiksi jäljittämään tietyn ajoneuvon liikettä risteyksessä. **SignalStatus, signalStatusPackage**: kuvaa vastausta etuuspyyntöihin ja mahdollisesti kirjaa vuorovaikutustiedot ja -tuloksen ajoneuvojen tai pyytäjien osalta.
CAM Cooperative Awareness Message	CAM-viesti tarjoaa ajoneuvo- tai tapahtumatietoja liikenteen infrastruktuurille (V2I). Tietoja voidaan välittää myös ajoneuvosta toiseen (V2V), mutta spesifikaatio ei vielä ota niihin kantaa. **Station ID**: C-ITS-yksikön yksilöllinen tunniste. **Reference Position**: ajoneuvon tarkka paikkatieto. **Speed and Heading**: ajoneuvon nopeus ja suunta. **Vehicle Length, Role and Type**: tietoja ajoneuvon tyypistä, perävaunuista, mitoista, roolista ja esim. sireenin käytöstä. **Timestamp**: tietojen aikaleima.

C-ITS-viestiprofiili	Esimerkkejä tietosisällöstä, joka saattaa sisältää henkilötietoa
CPM Collective Perception Message	CPM-viesti tarjoaa tietoa ajoneuvon antureiden havaitsemista objekteista muille tienkäyttäjille sekä liikenneinfralle. **Originating ITS-S Information**: sisältää tietoja lähettävästä ajoneuvosta tai muusta C-ITS-yksiköstä. **Sensor Information**: sisältää tietoa käytössä olevien antureiden kokoonpanosta ja ominaisuuksista. **Detected Objects**: dynaamista tietoa ympäristöstä havaituista kohteista, ml. kohteen ID, sijainti, nopeus ja luokittelu. **Timestamp and Positional Data**: Kohteen havaintoaika ja -paikka.

8.3.3 Yksityisyyden suoja pitkän kantaman tiedonsiirrossa

Yksityisyyden suojaa C-ITS:n pitkän kantaman tiedonsiirtoratkaisussa koskevat vaatimukset on harkittu huolellisesti, mutta niihin liittyy tiettyjä haasteita. Pseudonymisointi ja tunnisteiden säännöllinen vaihtaminen vähentävät seurantamahdollisuuksia pitkällä aikavälillä ja ovat keskeinen menetelmä yksityisyyteen liittyvien riskien vähentämiseksi. Henkilöitä yksilöivät tiedot säilytetään yleensä vain lyhyitä aikoja, tyypillisesti enintään viisi minuuttia, jotta tietojen anonymiteetti maksimoidaan. Lisäksi turvamekanismit kuten varmenteet ja salaus (ETSI TS 103 097) suojaavat viestien eheyttä ja aitoutta.

Tästä huolimatta erityisiä yksityisyyteen liittyviä huolenaiheita on edelleen, ja ne liittyvät erityisesti ajoneuvojen jäljitettävyyteen pseudonymisoinnista huolimatta sekä verkottuneiden ajoneuvojärjestelmien integroimiseen. Tämä korostaa tarvetta lisäarvioinnille ja mahdollisille sääntelymuutoksille teknologian kehittyessä, painottaen tasapainoa C-ITS-palveluiden hyötyjen ja yksityisyyden suojaa koskevien vaatimusten välillä. Olemassa olevat menetelmät tarjoavat vahvan perustan, mutta jatkuvia päivityksiä ja parannuksia tarvitaan vastaamaan erityisesti pitkän kantaman tiedonsiirrossa käytettävissä viesteissä syntyviin uusiin haasteisiin yksityisyyden suojan takaamiselle.

C-ITS-järjestelmissä IP-pohjaista viestintää käytetään pitkän kantaman tiedonsiirtoon, erityisesti taustajärjestelmien välillä sekä infrastruktuurin ja ajoneuvon tietopalveluissa (I2V). Tämä mahdollistaa hallitun tietojen jakamisen, mutta tähän liittyy tiettyjä tietosuojaongelmia. IP-osoitteet ovat muita tietojoukkoja yhdistelemällä yhdistettävissä C-ITS-yksiköihin ja siitä ajoneuvoihin ja henkilöihin tai suoraan luonnollisiin henkilöihin.

Pseudonymisoidut tunnisteet parantavat yksityisyyden suojaa, mutta riski yksittäisen henkilön tunnistamisesta jää jäljelle, jos tunnistamista yrittävän toimijan käytettävissä on riittävästi lisätietoja C-ITS-palveluiden ulkopuolisista lähteistä. C-ITS-palveluissa muodostuvien tietojen säilytyskäytännöissä määrätään, että mitään yksittäisen henkilön tunnistamisen mahdollistavia tietoja, kuten C-ITS-viesteihin liitettyjä varmenteita ja tunnisteita, ei tulisi säilyttää viittä minuuttia pidempään tietojen anonymiteetin säilyttämiseksi. Mahdollisuus yksityisyyden

loukkaamiseen seurannan tai luvattoman tietojen käytön seurauksena on tunnustettu huoli, johon on vastattu järjestelmän suunnittelussa mm. jatkuvalla pseudonyymien vaihdolla ja tiukoilla tietojen säilytyskäytännöillä.

Pitkän kantaman tiedonsiirtoratkaisussa C-ITS-viestit lähetetään IP-pohjaisessa verkossa TLS-protokollan tarjoamaa salausta hyödyntäen. Ratkaisu on kuvattu tarkemmin luvussa 6.3. PKI-allekirjoitus on salattuna TLS-protokollan mukaisen kuoren sisällä. Viestien välittäminen IP-pohjaisessa verkossa mahdollistaa hallitun ja turvallisen tietojen jakamisen hyödyntämällä X.509-varmenteita ja AMQP-protokollaa viestien reitityksessä. Tämä minimoi mahdollisuudet tietojen luvattomaan käyttöön tai ulkopuolisten mahdollisuudet hyödyntää viestien tietosisältöä C-ITS-palveluiden käyttäjien seurantaan. Vaikka pseudonyymejä tunnisteita voidaan käyttää yksityisyyden parantamiseksi, IP-pohjainen viestintä ei täysin poista yksityisyyden suojaan liittyviä riskejä, koska pseudonyymit voidaan silti mahdollisesti yhdistää yksilöihin, jos lisätietoja on saatavilla. C-ITS-järjestelmä on suunnittelu pienentämään näitä riskejä vaihtamalla pseudonyymejä usein ja rajoittamalla henkilötietojen säilyttämisen hyvin lyhyiksi ajoiksi.

C-ITS-keskusyksiköiden välisessä viestinnässä on käytössä EU:n C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukainen allekirjoitus. C-Roads-profiilispesifikaatiot eivät toistaiseksi ota kantaa siihen, miten IP-pohjaiset I2V- tai V2I-viestit välitetään loppukäyttäjän ja C-ITS-keskusyksikön välillä, mutta V2I-viesteissä välitetään lähes poikkeuksetta aika- ja paikkatietoa. I2V-viestit on puolestaan kyettävä kohdentamaan IP-pohjaisen verkon kautta vastaanottajan mobiililaitteeseen, joten pitkän kantaman tiedonsiirtoratkaisuissa viestien sisältö on syytä käsitellä henkilötietona.

Taulukossa 15 on vertailtu eri C-ITS-viestityyppien sisältämiä henkilötietoja lyhyen ja pitkän kantaman tiedonsiirtoratkaisuissa sekä viestien kulkusuunnan (I2V ja V2I) vaikutusta henkilötietojen muodostumiseen. DENM-viesteissä on huomioitu myös V2V-viestit. Tarkalleen ottaen henkilötietoa on vain sellainen tieto, joka on yhdistettävissä luonnolliseen henkilöön. Näin ollen pelkkä ajoneuvon aika- ja paikkatieto ei ole henkilötietoa, jos sitä ei voida yhdistää luonnolliseen henkilöön. Yhdistäminen vaatii lisätietoja, joten taulukossa on käytetty ilmaisua *'Voi syntyä henkilötietoa*'.

Taulukko 15. Eri C-ITS-viestityyppien henkilötiedot lyhyen ja pitkän kantaman kommunikoinnissa sekä viestien kulkusuunnan (I2V ja V2I) vaikutusta henkilötietojen muodostumiseen. DENM-viesteissä huomioitu myös V2V-viestit.

C-ITS-viesti	V2I (Vehicle to Infra)		I2V (Infra to Vehicle)	
	Lyhyt kantama	**Pitkä kantama**	**Lyhyt kantama**	**Pitkä kantama**
DENM (Hazardous Location Notification & Roads Works Warning)	Ei käytössä V2I-viesteissä. HUOM! **V2V-viesteissä** yksilöllinen tunniste ja tarkkaa paikkatietoa → **Voi syntyä henkilötietoa.**	Ei käytössä V2I-viesteissä. HUOM! **V2V-viesteissä** yksilöllinen tunniste ja tarkkaa paikkatietoa → **Voi syntyä henkilötietoa.**	C-Roads määritelmän mukaan → **Ei henkilötietoa**	Viestin sisältö ei ole henkilötietoa. Allekirjoitus ei ole henkilötietoa. Teleoperaattori tietää liittymän sijainnin, joten yhdistelemällä → **Voi syntyä henkilötietoa.**
IVIM (In-Vehicle Signage & Automated Vehicle Guidance)	Ei käytössä	Ei käytössä	C-Roads määritelmän mukaan → **Ei henkilötietoa**	Viestin sisältö ei ole henkilötietoa. Allekirjoitus ei ole henkilötietoa. Teleoperaattori tietää liittymän sijainnin, joten yhdistelemällä → **Voi syntyä henkilötietoa.**
SPATEM, MAPEM (Signal phase and timing, traffic light priority, Emergency vehicle priority...)	Ei käytössä. Ajoneuvo hyödyntää paikkatietoaan, mutta tietoa ei välitetä ulospäin.	Ei käytössä. Ajoneuvo hyödyntää paikkatietoaan, mutta tietoa ei välitetä ulospäin.	C-Roads määritelmän mukaan → **Ei henkilötietoa**	Viestin sisältö ei ole henkilötietoa. Allekirjoitus ei ole henkilötietoa. Teleoperaattori tietää liittymän sijainnin, joten yhdistelemällä → **Voi syntyä**

				henkilötietoa.
C-ITS-viesti	**V2I (Vehicle to Infra)**		**I2V (Infra to Vehicle)**	
	Lyhyt kantama	**Pitkä kantama**	**Lyhyt kantama**	**Pitkä kantama**
SSEM, SREM	Priorisoitu ajoneuvo lähettää priorisointipyynnön. Sisältää ajoneuvon aika ja paikkatietoa. → **Voi syntyä henkilötietoa.** Max säilytysaika 5 min.	Priorisoitu ajoneuvo lähettää priorisointipyynnön. Sisältää ajoneuvon aika ja paikkatietoa → **Voi syntyä henkilötietoa.** Max säilytysaika 5 min.	C-Roads määritelmän mukaan → **Ei henkilötietoa**	Viestin sisältö ei ole henkilötietoa. Allekirjoitus ei ole henkilötietoa. Teleoperaattori tietää liittymän sijainnin, joten yhdistelemällä → **Voi syntyä henkilötietoa.**
CAM (Probe Vehicle Data, Vehicle data collection, Event data collection)	V2I-tietoja. V2V-tietoihin ei vielä oteta kantaa. Välitetään monipuolista tietoa ajoneuvosta ja sen sijainnista. → **Voi syntyä henkilötietoa**. Max säilytysaika 5 min.	V2I-tietoja. V2V-tietoihin ei vielä oteta kantaa. Välitetään monipuolista tietoa ajoneuvosta ja sen sijainnista. → **Voi syntyä henkilötietoa**. Max säilytysaika 5 min.	Ei käytössä	Ei käytössä
CPM	V2I-tietoja. V2V-tietoihin ei vielä oteta kantaa. Välitetään monipuolista tietoa ajoneuvosta ja sen sijainnista. → **Voi syntyä henkilötietoa**. Max säilytysaika 5 min.	V2I-tietoja. V2V-tietoihin ei vielä oteta kantaa. Välitetään monipuolista tietoa ajoneuvosta ja sen sijainnista. → **Voi syntyä henkilötietoa**. Max säilytysaika 5 min.	Ei käytössä	Ei käytössä

8.3.4 Yhteenveto C-ITS-viestien sisältämistä henkilötiedoista

C-ITS-yksiköt sisällyttävät viestiinsä tyypillisesti oman yksilöllisen tunnisteensa. Ajoneuvo voi toimia C-ITS-yksikkönä, joten sen lähettäessä tietoa yksilöllinen tunniste kulkee viestin mukana. Yllä olevan analyysin mukaisesti tämä tunniste tai C-ITS-viestit yleensä eivät sisällä henkilötiedoksi määriteltyä tietoa, kuten tietoja kuljettajasta, katuosoitetta, rekisterinumeroa tai ajoneuvon VIN-koodia. Myöskään erityisiä henkilöryhmätietoja (etninen alkuperä, uskonto, terveys, jne.) niissä ei välitetä.

Erilaista aika- ja paikkatietoa, C-ITS-yksiköiden välisessä viestinnässä käytettäviä pseudonymisoituja tunnisteita ja IP-osoitteita puolestaan välitetään hyvinkin monipuolisesti. C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaiset C-ITS-viestit ovat julkisen avaimen menetelmällä allekirjoitettuja. Julkisen avaimen menetelmällä toteutettujen allekirjoitusten käyttö C-ITS-järjestelmissä ei tee viesteistä anonyymejä, sillä allekirjoituksissa käytetyt varmenteet voidaan silti liittää tiettyihin käyttäjiin tai ajoneuvoihin juurivarmentajan käyttämillä alivarmentajilla (EA, Enrollment Authority ja AA, Authorisation Authority) olevien tietojen avulla.

C-ITS-järjestelmät on suunniteltu siten, ettei palveluiden käyttäjiä pystytä jäljittämään. Jäljittämisen estämiseksi järjestelmissä käytetään lyhytaikaisia, usein vaihtuvia valtuutuslippuja ja rajoittamalla pseudonymisoitujen tietojen säilytysaika hyvin lyhyeksi. Tämä lähestymistapa vähentää pitkäaikaisen seurannan riskiä ja perustuu yksityisyyden suojan periaatteisiin. Vaikka pseudonyymisyys ei vastaa täyttä anonymiteettiä, se rajoittaa merkittävästi kykyä jäljittää ja yhdistää viestejä yksittäisiin käyttäjiin ilman lisätietoa, mikä vastaa GDPR:n vaatimuksia henkilötietojen suojaamiseksi.

Lyhyen ja pitkän kantaman tiedonsiirrossa käytettävien viestien rakenne on tarkemmin kuvattu luvussa 6.3.1. Lyhyen kantaman tiedonsiirron viestejä voi kuka tahansa lähettää ja vastaanottaa annetulla taajuuskaistalla. Lyhyen kantaman tiedonsiirron I2V-viestien sisältämä aika- tai paikkatieto ei sinänsä synnytä henkilötietoa, koska lähettäjä ei kykene identifioimaan vastaanottajaa. C-ITS-tienvarsiyksiköiden ja C-ITS-keskusyksiköiden viestinnässä ajoneuvoihin ja tienkäyttäjiin päin tietosuojaa ei pidetä tärkeänä, koska I2V-tyyppisissä palveluissa ei käsitellä henkilötietoja (C-ITS Security & Governance, 2023, 15).

Julkisen avaimen menetelmällä allekirjoitetun varmenteen käyttäminen erityisesti V2I-viesteissä saattaa muuttaa tilanteen. Varmenne on pseudonymisoitua tietoa ja siten vastaanottaja on identifioitavissa mahdollisen lisätiedon avulla. Esimerkiksi lyhyen kantaman tiedonsiirrossa V2I-viestit (esim. käyttötapaus Probe Vehicle Data, PVD) välittävät ajoneuvon tietoja toisten ajoneuvojen ja infran suuntaan, joten siinä saattaa muodostua henkilötietoa. Varmenteen lisäksi myös muut C-ITS-viestiin sisältyvät tiedot saattavat yksilöidä C-ITS-yksikön. Esimerkiksi IEEE 802.11p -kehykseen sisältyvä MAC-osoite saattaa olla tällainen tieto.

C-ITS-järjestelmän suunnittelussa GDPR ja yksityisyyden suoja on otettu vakavasti, ja sen periaatteet on laajasti sisällytetty järjestelmän toimintaperiaatteisiin. Pseudonymisointi on keskeinen strategia yksityisyyteen liittyvien riskien vähentämiseksi vaihtamalla käyttäjäidentiteettejä säännöllisesti, mikä vähentää seurantamahdollisuuksia pitkällä aikavälillä. C-ITS-viestien voidaan sanoa noudattavan

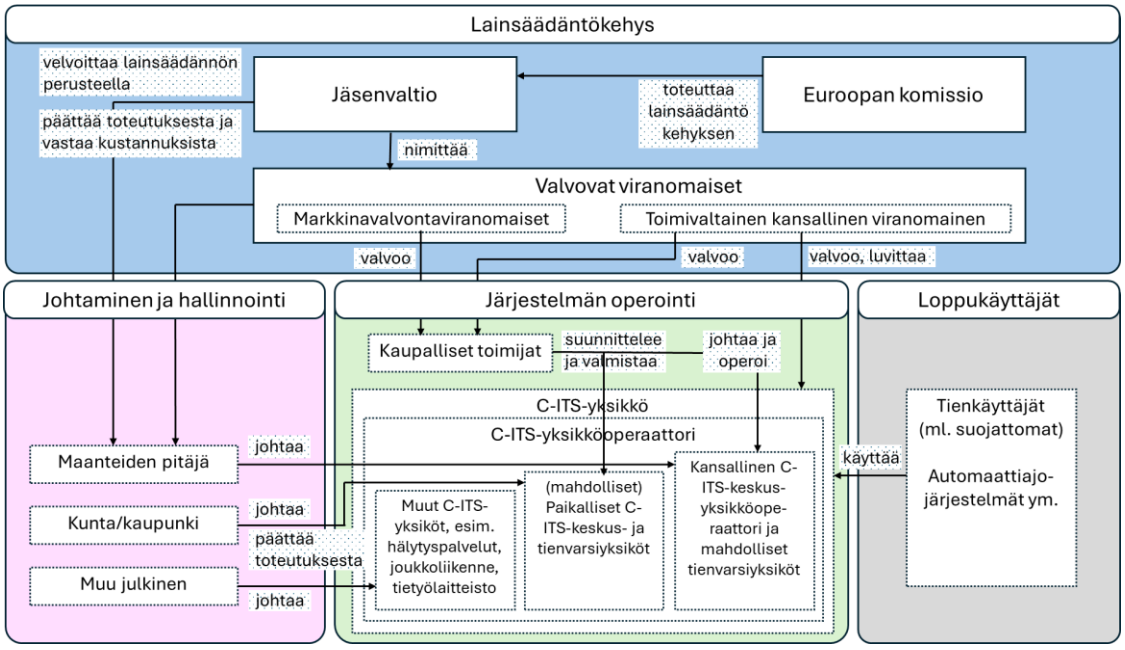
GDPR:n tietosuojaperiaatteita, mutta luonteeltaan erityisesti välitettävä V2I-tieto on henkilötietoa ja sellaisena sitä on kohdeltava.

8.4 Tieto- ja yksityisyyden suoja suomalaisessa toteutusmallissa

8.4.1 Viranomaisten roolit C-ITS-palveluiden käyttöönotossa ja käytössä

Traficomin julkaisussa *"Viranomaisten roolit vuorovaikutteisten älykkäiden liikennejärjestelmien (C-ITS) palveluiden käyttöönotossa ja operatiivisessa käytössä*" (Kotilainen et al. 2023) on käsitelty viranomaisten rooleja C-ITS-palveluiden käyttöönotossa ja operatiivisessa käytössä Suomessa. Raportissa hyödynnetään C-Roads WG1-työryhmän raportissa esitettyä standardin ISO TS 17427 mukaista arkkitehtuurikuvausta C-ITS:n liittyvien roolien ja vastuiden organisoinnista. Raportti korostaa viranomaisten ja muiden toimijoiden hyvää roolijakoa eri tehtävissä.

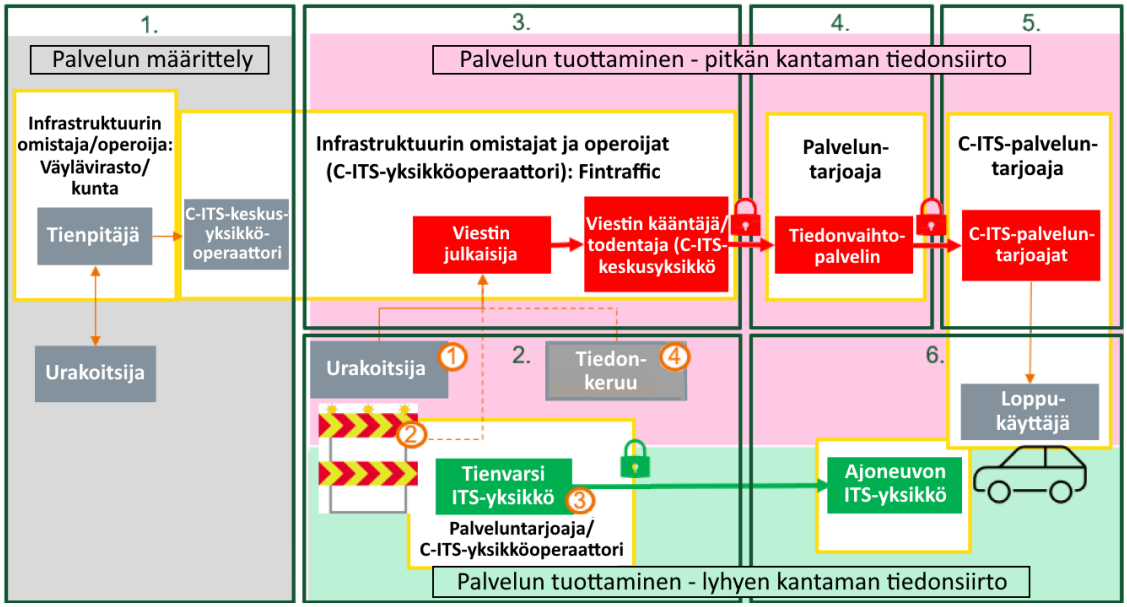
Ehdotetussa järjestelyssä Traficom toimii keskeisenä markkinavalvontaviranomaisena, joka vastaa C-ITS-yksiköiden vaatimustenmukaisuuden arvioinnista sekä turvallisuuden valvonnasta yhteistyössä Turvallisuus- ja kemikaaliviraston (TUKES) kanssa. Väylävirasto ja kunnat toimivat infrastruktuurin omistajina ja operoijina vastaten esimerkiksi tiedonsiirtoverkon ylläpidosta ja tienvarsiyksiköiden hallinnasta. Roolijakoa on kuvattu tarkemmin kuvassa 13.



Kuva 13. Viranomaisten roolijako C-ITS-palveluiden käyttöönotossa ja operatiivisessa käytössä Suomessa (mukaillen Kotilainen et al. 2023).

Raportissa on käsitelty kahden C-ITS-palvelun roolijakoa. Mukana ovat (i) Tietyövaroitus ja sen käyttötapauksena kaistan sulkeminen (Road Works Warning, RWW) sekä (ii) Liikennevalot käyttötapauksena opastimen tilatieto ja liikennevalojen ajoitus (Signal Phase and Timing Information, SI-SPTI).

Käyttötapauksen kaistan sulkeminen tuottamiseen liittyvät operatiiviset roolit on esitetty kuvassa 14.



Kuva 14. Tietyövaroitus-palvelun suljettu kaista -käyttötapauksen operatiiviset roolit (Kotilainen et al. 2023).

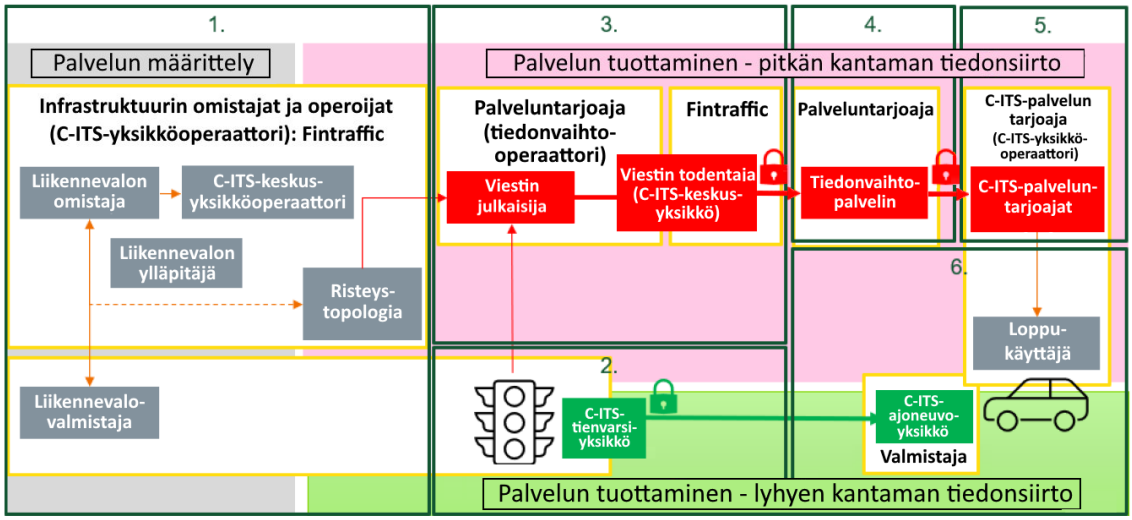
Kuvan 14 mukaisessa roolituksessa urakoitsija sopii infrastruktuurin omistajan kanssa, miten tietyövaroitus tuotetaan. Pitkän kantaman tiedonsiirtoratkaisussa on mahdollista hyödyntää Fintraffic Tie Oy:n ylläpitämää Tietyöilmoituspalvelua tai integroida tietyöperävaunuun C-ITS-yksikkö, joka matkaviestinverkon tai lähiverkon välityksellä ilmoittaa tilansa viestin julkaisijalle.

Yksityisyyden suojaa eri rooleissa ja tiedonsiirtovaihtoehdoissa (käyttötapaus suljettu kaista, I2V) on tarkasteltu taulukossa 16.

Taulukko 16. Yksityisyyden suoja eri tehtävissä ja tiedonsiirtovaihtoehdoissa, kun kyseessä on tietyövaroitus-palvelun suljettu kaista -käyttötapauksen käsittely (mukaillen Kotilainen et al. 2023).

Tehtävä ja toimija	Lyhyt kantama	Pitkä kantama
Palvelun määrittely. Tietyön tilaaja (Väylävirasto, kunta, jne.)	Tässä vaiheessa ei C-ITS-henkilötietoa synny. Sopimuksessa määritellään tapauskohtaisesti mm. tiedonvaihtotapa, viestintäteknologiat, tienvarsiyksiköt ja palvelut sekä tiedon laatuvaatimukset. Lisäksi sovitaan, kuka julkaisee ja todentaa viestit. Vaihe määrittää mahdollisen rekisterinpitäjän.	
Tietyövaroituksen tuottaja (urakoitsija). C-ITS-yksikköoperaattori vastaa C-ITS-yksiköiden tietoturvasta.	Urakoitsija käyttää tietyöperävaunuun integroitua C-ITS-yksikköä. Kyseessä on I2V-tyyppinen tieto, joten lähettäjälle ei synny henkilötietoa. Mahdollinen yhdisteltävyys esim. työvuorolistoihin on estettävä. C-ITS-yksikköoperaattoria koskevat ISO 27001/NIS2 mukaiset velvoitteet.	Urakoitsija käyttää tietyöperävaunuun integroitua C-ITS-yksikköä ja matkaviestinverkkoa tai välittää tiedot julkaisijalle (esim. Fintraffic). Kyseessä on I2V-tyyppinen tieto, joten lähettäjälle ei synny henkilötietoa. Mahdollinen yhdisteltävyys esim. työvuorolistoihin on estettävä. C-ITS-yksikköoperaattoria koskevat ISO 27001/NIS2 mukaiset velvoitteet.
Viestin julkaisu ja varmennus (C-ITS-keskusyksikkö, kansallinen tai kunnan yhteyspiste).	Ei käytössä.	Kyseessä on C-ITS-keskusyksikkö tai kansallinen yhteyspiste (NAP) eli esim. Fintraffic tai urakoitsija. Vastaanotettu tieto on I2V-tyyppistä tietoa, joka ei sisällä henkilötietoa. Mahdollinen yhdisteltävyys esim. työvuorolistoihin on estettävä. C-ITS-keskusyksikköoperaattoria koskevat ISO 27001/NIS2 mukaiset velvoitteet ja ne ovat vastuussa lähtötietojen luotettavuudesta.

Liikennevalojen käyttötapauksessa operatiiviset roolit on esitetty kuvassa 15, ja yksityisyyden suojaa eri rooleissa ja tiedonsiirtovaihtoehdoissa (SI-SPTI-viesti, I2V) on tarkasteltu taulukossa 17.



Kuva 15. Opastimien tilatieto ja liikennevalojen ajoitusta koskeva tieto (Signal Phase and Timing Information) -käyttötapauksen operatiiviset roolit. (mukaillen Kotilainen et al. 2023).

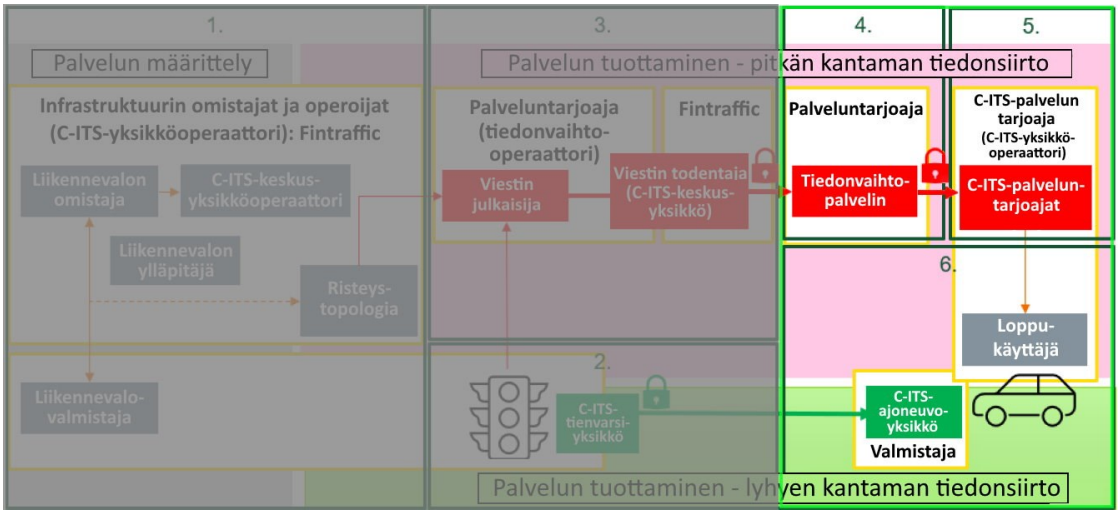
Yksityisyyden suojaa eri rooleissa ja tiedonsiirtovaihtoehdoissa (Signal Phase and Timin Information, I2V) on tarkasteltu taulukossa 17.

Taulukko 17. Yksityisyyden suoja eri tehtävissä ja tiedonsiirtovaihtoehdoissa, kun kyseessä on liikennevalojen SI-SPTI viestin käsittely (mukaillen Kotilainen et al. 2023).

Tehtävä ja toimija	Lyhyt kantama	Pitkä kantama
Palvelun määrittely. Infrastruktuurin omistaja (Väylävirasto, Fintraffic, ELY, kunta)	Tässä vaiheessa ei henkilötietoa synny. Sopimusvaiheessa liikennevalojen infrastruktuurin omistaja(t), liikennevalojen ylläpitäjä ja C-ITS-palveluntarjoajana toimiva operaattori sopivat tiedonvaihdosta ja siitä, miten kaksi erityypistä viestiä (SPATEM ja MAPEM) välitetään. Infrastruktuurin omistaja hankkii laitteet liikennevalovalmistajalta. Sopimusvaiheessa osapuolet sopivat, miten SPATEM- ja MAPEM-viestit välitetään.	
Liikennevalot (Liikennevalolaitevalmistaja)	C-ITS-yksikkö välittää tiedot C-ITS-viestinä. Yksikön operoinnista ja tietoturvasta vastaa C-ITS-yksikköoperaattori (esim. Fintraffic tai kunta). Radioteknologian vaatimustenmukaisuudesta vastaa Traficom. Kyseessä on I2V-tyypinen tieto, joten lähettäjälle ei synny henkilötietoa. Lähettäjä allekirjoittaa viestin ja lähettää sen radioteitse suoraan loppukäyttäjälle.	Liikennevalon ohjauskoje lähettää SPATEM-viestin julkaisijalle. Viestiä ei vielä allekirjoiteta. I2V-tyyppinen viesti ei sisällä henkilötietoa.

	C-ITS-yksikköoperaattoria koskevat ISO 27001/NIS2 mukaiset velvoitteet.	
Tehtävä ja toimija	**Lyhyt kantama**	**Pitkä kantama**
Viestin julkaisu (Fintraffic, kunta, liikennevalovalmistajan järjestelmä)	Ei käytössä.	Viestin julkaisija, esim. Fintraffic, kunnan yhteyspiste tai liikennevalovalmistajan taustajärjestelmä, lähettää SPATEM- ja MAPEM-tietoa eteenpäin allekirjoittavaksi. Allekirjoitus ja lähetys tapahtuvat C-ITS-keskusyksikössä ja sen suorittavat esim. Fintrafficin tai liikennevalovalmistaja. Vastaanotettu liikennevalotieto on I2V-tyyppistä tietoa, joka ei sisällä henkilötietoa. C-ITS-keskusyksikköoperaattoria koskevat ISO 27001/NIS2 mukaiset velvoitteet. Se on vastuussa lähtötietojen luotettavuudesta.

Molemmille käyttötapauksille kuvatut yhteiset roolit on esitetty kuvassa 16, ja yksityisyyden suojaa näissä eri rooleissa ja tiedonsiirtovaihtoehdoissa on tarkasteltu taulukossa 18.



Kuva 16. Molemmille käyttötapauksille kuvatut yhteiset operatiiviset roolit (mukaillen Kotilainen et al. 2023).

Taulukko 18. Yksityisyyden suoja eri käyttötapauksissa niiden yhteisten toimintojen osalta (mukaillen Kotilainen et al. 2023).

Tehtävä ja toimija	Lyhyt kantama	Pitkä kantama
Tiedonvaihtopalvelin (Fintraffic, kunta, C-ITS-palveluntarjoaja)	Ei käytössä	Välittää allekirjoitettuja C-ITS-viestejä C-ITS-palveluntarjoajille. Käsittely perustuu AMQP-protokollan otsikkoon. Ei allekirjoita viestejä. Käsiteltävä tieto on I2V-tyyppistä tietoa, joka ei sisällä henkilötietoa. Mahdollinen yhdisteltävyys esim. työvuorolistoihin on estettävä. ISO 27001 -velvoitteet eivät koske, mutta NIS2-direktiivin velvoitteet koskevat.
Yksityinen tai julkinen C-ITS-palveluntarjoaja	Ei käytössä	Tilaa käyttämänsä C-ITS-viestit alueelta, jossa palvelun käyttäjät liikkuvat. Tarkastaa viestin varmenteen ja lähetysoikeudet. Lähettää viestin loppukäyttäjälle oman ratkaisunsa mukaisilla keinoilla, eikä tältä osin ole osa EU:n C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS). I2V-tyyppinen viesti itsessään ei sisällä henkilötietoa, mutta palveluntarjoajalla on asiakkaastaan muuta henkilötietoa ja rekisterinpitäjän rooli. Käsittelyperusteena kaupalliset toimijat käyttävät tyypillisesti oikeutettua etua (asiakassuhde) tai sopimussuhdetta.
Loppukäyttäjä (ajoneuvon kuljettaja, automaattiajojärjestelmä, suojaton tienkäyttäjä)	Ajoneuvon C-ITS-yksikkö. Tarkistaa viestin varmenteen. Ei sisällä henkilötietoa. Ei erityisiä vaatimuksia loppukäyttäjälle.	C-ITS-palvelun tuottajan tarjoama keino esim. mobiilisovellus. Ei erityisiä vaatimuksia loppukäyttäjälle.

Kotilainen et al. (2023) suosittelevat raportissaan perustamaan kansallisella tasolla koordinaatioryhmiä, jotka koostuvat valtion, kuntien ja yksityisten toimijoiden edustajista. Nämä ryhmät keskittyvät C-ITS-palveluiden määrittelyyn ja näiden palveluiden jatkuvaan kehittämiseen teknologian edetessä. Lisäksi kansalliseksi viranomaiseksi ehdotetaan toimivaltaista yksikköä, joka myöntäisi luvat erityisviestejä lähettäville C-ITS-yksiköille, kuten hälytysajoneuvoja varten.

Mikäli palvelut toteutetaan kansallisesti, Fintraffic Tie Oy:llä on keskeinen rooli C-ITS-keskusyksikköoperaattorina, ja sillä on vastuu viestien julkaisemisesta ja varmentamisesta. Raportissa korostetaan erilaisten ratkaisuiden, kuten pitkän ja lyhyen kantaman tiedonsiirron käyttöä ja niiden hallintaa erilaisten toimijoiden, kuten urakoitsijoiden ja C-ITS-yksikköoperaattorien, kautta.

Kokonaisuuden kannalta olennaista on viranomaisten, yksityisten toimijoiden ja loppukäyttäjien välinen koordinointi, jotta C-ITS-järjestelmiä voidaan kehittää ja valvoa tehokkaasti ja turvallisesti sekä kansallisesti että eurooppalaisella tasolla.

8.4.2 Valvova viranomainen

Tietosuojan kansallinen valvontaviranomainen on tietosuojavaltuutettu. Markkinavalvontaviranomaisena toimii Liikenne- ja viestintävirasto Traficom. Sen tehtävänä on valvoa sähköisiä viestintä- ja liikennepalveluita liittyen kuluttajien oikeuksiin ja markkinoiden toimivuuteen. Traficom puuttuu epäkohtiin kuten kilpailun vastaisiin käytäntöihin tai kuluttajien oikeuksia loukkaaviin toimintoihin, mutta ei ole keskittynyt henkilötietojen suojaan samassa laajuudessa kuin tietosuojavaltuutettu.

8.4.3 Hallinnointi ja johtaminen

Tietosuojalainsäädännön vaikutukset: rekisterinpitäjän roolissa johtamisen ja päätöksenteon tukena on velvollisuutena tehdä tietosuojan vaikutustenarviointi ja laatia seloste käsittelytoimista, jonka avulla kykenee tiedottamaan rekisteröityä henkilötietojen käsittelystä ja hänen oikeuksistaan.

8.4.4 Yhteenveto tietosuoja- ja tietoturvavaatimusten täyttämisestä Suomessa

Jos C-ITS-palvelut otetaan käyttöön viranomaisten roolit C-ITS-palveluissa raportissa (Kotilainen et al. 2023) kuvattujen organisaatioiden ja teknologioiden avulla, EU:n tietosuoja- ja tietoturvavaatimusten täyttäminen Suomessa edellyttää seuraavia toimenpiteitä:

- EU:n yleisen tietosuoja-asetuksen (GDPR) mukaista henkilötietojen käsittelyä viestien välittämiseen ja tallentamiseen osallistuvissa organisaatioissa kuten Fintraffic, kunnat ja yksityiset toimijat.
- C-ITS-operaattoreilta edellytetään standardin ISO 27001 mukaista sertifioitua tietoturvallisuuden hallintajärjestelmää (yksityinen sektori) tai NIS1- ja NIS2-kyberturvallisuusdirektiivien mukaisten vaatimusten soveltamista (tienpitäjät).
- Luvussa 5 kuvatun C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaiset kansalliset puitteet varmennettujen tietojen vaihtamiseen C-ITS-yksiköiden välillä.

- C-ITS-yksiköiden turvallisuuden arviointiin ja sertifiointiin tarvitaan SOG-IS-vaatimustenmukaisuuden arviointielin. Suomessa ei tällaista arviointielintä ole, mutta muissa maissa olevia arviointielimiä voidaan hyödyntää MRA-sopimuksen (Mutual Recognition Agreement) vastavuoroisen tunnustamisen periaatteiden mukaisesti koko Euroopassa.
- Eri viranomaisten, kuten Traficomin ja Väyläviraston, sekä yksityisten toimijoiden, kuten kaupallisten palveluntarjoajien, roolien selkeämpi määrittely. Tarve on selkeille sopimuksille ja määrittelyille, miten kustannukset ja operointivastuut sekä infrastruktuurin omistus, hallinta ja ylläpito jaetaan eri toimijoiden kesken, erityisesti kun palvelut ylittävät kansallisia rajoja.

8.4.5 Järjestelmän operointi

Tietosuojalainsäädännön vaikutukset: rekisterinpitäjän lukuun operaattorina tehtävät toimet kuvataan henkilötiedon käsittelijän selosteessa. Selosteella tiedotetaan rekisteröityä henkilötietojen käsittelystä ja hänen oikeuksistaan.

Henkilötietojen käsittelijän on avustettava tarvittaessa rekisterinpitäjää tietosuojan vaikutustenarvioinnin tekemisessä. Lisäksi henkilötietojen käsittelijä ilmoittaa rekisterinpitäjälle henkilötietojen tietoturvaloukkauksista sekä huolehtii asianmukaisesta tietoturvasta, tietojen tuhoamisesta sekä osallistuu auditointeihin.

8.4.6 Loppukäyttäjä

Tietosuojalainsäädännön vaikutukset: rekisteröidyn oikeudet täyttyvät ja oikeuksien käyttäminen helpottuu. Rekisterinpitäjän tekemän tietosuojan vaikutustenarvioinnin perusteella on tunnistettu mahdolliset riskit rekisteröidylle, ja rekisteröidyllä tulisi olla mahdollisuus päättää jakaako henkilötietonsa C-ITS-palvelulle.

8.5 Yhteenveto ja suositukset

C-ITS-palveluissa on kiinnitetty paljon huomiota yksityisyyden suojan toteutumiseen, ja puuttuvasta C-ITS-asetuksesta huolimatta useissa eri EU-maissa on lähtenyt liikkeelle C-ITS-toteutuksia. Tästä huolimatta on todettava, että EU:n yleisen tietosuoja-asetuksen (GDPR) periaatteiden toteuttamiseen sekä henkilötietojen ja yksityisyyden suojan toteuttamiseen liittyviä kysymyksiä ei ole vielä lopullisesti ratkaistu.

8.5.1 Riskienhallinta

Tietosuojan periaatteiden mukaan rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyviä riskejä aina ennen, kuin se ryhtyy käsittelemään henkilötietoja. Tietosuojan vaikutustenarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Se on tarkoitettu jatkuvaksi riskien tunnistamisen ja hallitsemisen prosessiksi.

EU:n yleinen tietosuoja-asetus (GDPR) ei nimenomaisesti vaadi siirtovaikutusten arviointia erillisenä käsitteenä, mutta EU:n tietosuojaviranomaiset ja Euroopan tietosuojaneuvosto (EDPB) ovat korostaneet sen tärkeyttä osana GDPR:n velvoitteiden täyttymistä. Erityisesti tilanteissa, joissa henkilötietoja siirretään EU/ETA-alueen ulkopuolelle ilman riittävyyspäätöstä, siirtovaikutusten arviointi nähdään osana asianmukaisten suojatoimenpiteiden käyttöönottoa ja riskienhallintaa.

Henkilötietojen tietoturvaloukkaustapahtumassa rekisterinpitäjällä on velvollisuus arvioida tapahtuman riskitaso ja sen mukaisesti dokumentoida tapahtuma ja ilmoittaa valvovalle viranomaiselle. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille.

Yksityisyyden suojan ja tietosuojan periaatteiden lisäksi kansallisessa lainsäädännössä velvoitetaan hävittämään tai pseudonymisoimaan sähköiset viestit ja välitystiedot. Pseudonymisoinnilla voidaan vähentää henkilötiedoista aiheutuvia riskejä muuntamalla henkilötietoja keinotekoisilla tunnisteilla siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja.

Tietosuojan arviointi- ja käsittelyprosessi määritellään tietoturvallisuuden hallintajärjestelmän standardin (ISMS, ISO/IEC 27001) tietosuojalaajennoksen ISO/IEC 27701 (PIMS, Tietosuojan hallintajärjestelmä) osion 5.4 (Suunnittelu) avulla. Tietosuojan arviointi- ja käsittelyprosessissa tunnistetaan henkilötiedon käsittelyyn liittyvät riskit. Tietoturvan hallintajärjestelmän osiota 8 (Toiminta) sovelletaan tietosuojan hallintajärjestelmään ilman lisävaatimuksia riskien asianmukaiseen hallinnointiin.

Riskienhallinnan velvoitteet tulevat monista eri lähteistä, jotka yhdessä muodostavat kattavan viitekehyksen organisaatioiden tietosuojakäytäntöjen kehittämiseen ja ylläpitoon. EU-tietosuojalainsäädäntö asettaa rekisterinpitäjille ja henkilötietojen käsittelijöille velvoitteita tunnistaa ja hallita henkilötietojen käsittelyyn liittyviä riskejä. Kansallinen tietosuojalainsäädäntö täydentää EU-lainsäädännön vaatimuksia. Ne voivat sisältää erityisvelvoitteita, jotka vastaavat kyseessä olevan maan tietosuojan tai tietoturvan erityistarpeisiin. Hallintajärjestelmästandardit tarjoavat rakenteellisen lähestymistavan tietosuojan riskienhallintaan, määrittävät prosessit riskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi sekä menetelmät hallintakeinojen riittävyyden ja toimivuuden varmistamiseksi.

EU-tason ja kansallisen tietosuojalainsäädännön ohella standardit voivat tarjota organisaatioille konkreettisia prosesseja ja työkaluja lainsäädännön vaatimusten täyttämiseksi sekä jatkuvaksi parantamiseksi tietosuojakäytännöissä. Riskienhallinta vaatii jatkuvaa valvontaa, arviointia ja parantamista. Jatkuva parantaminen mahdollistaa organisaatioille sopeutumisen muuttuviin uhkiin ja uusiin tieto- ja henkilösuojausvaatimuksiin.

Kaikki nämä elementit tukevat monitasoista lähestymistapaa riskienhallintaan, jossa EU- ja kansalliset vaatimukset sekä standardit ohjaavat organisaatioiden toimintaa käytännön menetelmin. Yhteistyö ja integroitu lähestymistapa mahdollistavat systemaattisen riskien tunnistamisen, arvioinnin ja käsittelyn sekä auttavat organisaatioita pysymään vaatimustenmukaisina.

8.5.2 Kansallisen tai EU-tason sääntelyn puutteet

C-ITS-viestejä vaihtavan verkoston laajuus ja käsiteltävän henkilötiedon määrä on monessa yhteydessä nostettu erityiskysymykseksi, joka edellyttää delegoidun C-ITS-asetuksen laatimista ja hyväksyntää. Asetuksella tulee olla myös European Data Protection Board (EDPB) hyväksyntä. C-ITS-järjestelmiä ja C-ITS-palveluita koskevan lainsäädännön puuttuessa tilanne on monelta osin ristiriitainen, ja vakiintunutta oikeuskäytäntöä ei ole kyetty muodostamaan. Raportin kirjoittamisaikana ei ollut käytettävissä tietoja asetuksen tulevasta käsittelystä.

Erityisesti loppukäyttäjien kannalta käsittelyperuste, joka perustuu suostumukseen tai sopimukseen, on C-ITS-viestien osalta hankala toteuttaa. Oikeutettu etu puolestaan edellyttää yleensä tapauskohtaisia tasapainotestejä ja lisäsuojatoimenpiteitä, mikä on haastavaa laajassa valtakunnallisessa palvelussa.

Yleinen etu on erityisesti viranomaisten osalta hyvä ehdokas käsittelyperusteeksi. Yleisen edun käyttöä tulisi tukea kansallisella tai EU-lainsäädännöllä, joka vahvistaa käsittelyn tarpeellisuuden tietyn yleisen edun saavuttamiseksi. Tämä tarkoittaa, että käsittelyn on oltava kiinteästi sidottu tiettyyn demokraattisesti hyväksyttyyn tavoitteeseen tai yhteiskunnan tarpeeseen.

Käsittelyperusteen osalta vaikuttaa välttämättömältä, että C-ITS-palveluiden laajempi toteuttaminen edellyttää yleisen edun perusteiden (esim. liikenneturvallisuus) kirjaamista lakiin. Lainsäädännössä tulee selkeästi määritellä, mikä on yleinen etu ja miten henkilötietoja voidaan käsitellä tämän edun perusteella. Tämä voi sisältää tiedot siitä, kenen vastuulla käsittely on ja mitkä ovat käsittelyn rajoitteet ja ehdot. Liikenneturvallisuuden parantamista voitaneen käyttää yleisenä etuna, mutta tämän on oltava osa laajempaa lainsäädäntökehystä, joka tarkentaa, millaisissa tilanteissa ja millä edellytyksillä henkilötietojen käsittely on sallittua näiden tavoitteiden saavuttamiseksi. Tämä lienee toteutettavissa. Vaihtoehtoisesti C-ITS-palveluiden toteuttaminen voidaan kirjata lakisääteiseksi velvollisuudeksi, joten käsittelyperusteeksi muodostuu lakisääteinen velvollisuus. Toteuttaminen vaatinee laajempaa kansainvälistä yhteistyötä.

C-ITS-palveluiden käyttäjille on vaikea tiedottaa, miten heidän tietojaan käytetään. GDPR korostaa läpinäkyvyyttä ja käyttäjän oikeutta päästä tietoihinsa, joten näiden mekanismien ja lainsäädännön kehittäminen on tärkeää. Autojen hätäviestijärjestelmä eCallin yhteydessä asia ratkaistiin informoimalla asiasta ajoneuvon käyttöohjeessa. C-ITS:n osalta on esitetty kritiikkiä, että tämä ei riitä.

Parannettavaa kansallisesti

Suomessa tulisi toteuttaa useita toimenpiteitä C-ITS-palveluiden lainsäädännöllisten puutteiden korjaamiseksi. Olennaisinta on kehittää kansallista lainsäädäntöä linjassa EU:n tulevan C-ITS-asetuksen kanssa, mikä luo jäsenvaltioiden tasolla yhtenäiset pelisäännöt palveluiden toteutukselle. Tämä edellyttää, että Suomessa valmistellaan ja hyväksytään kansalliset lakimuutokset ITS-direktiivin (EU 2023/2661) ja muiden EU-säädösten mukaisesti. Lisäksi kansallisten viranomaisten ja ministeriöiden tulisi jatkaa aktiivista osallistumista EU-tason työryhmiin, kuten C-Roads Platform -yhteistyöryhmään, jotka pyrkivät yhdenmukaistamaan C-ITS-palveluiden käyttöönottoa jäsenvaltioissa.

Markkinavalvontaa ja tietoturvaa koskevat lait, kuten NIS2-direktiivin mukaiset säännökset, tulisi päivittää ajan tasalle vastaamaan kehittyviä turvallisuusvaatimuksia ja uuden teknologian tuomia haasteita. NIS2-direktiivi on tämän raportin kirjoitushetkellä eduskunnan käsittelyssä.

Hyvät ja toimivat käytännöt voivat osaltaan auttaa korvaamaan lainsäädännön puutteita. Yhteistyön vahvistaminen eri toimijoiden, kuten Väyläviraston, Fintraffic Tie Oy:n, Traficomin ja yksityisten palveluntarjoajien, välillä on tärkeää. Tämä yhteistyö voi osaltaan auttaa selkeyttämään vastuita ja toimintamalleja, jotka ovat välttämättömiä, jotta kaikki C-ITS-palvelut voidaan toteuttaa turvallisesti ja tehokkaasti.

Alan lainsäädäntö ja teknologia kehittyvät nopeasti. Jotta C-ITS-palveluiden sääntely on aina ajan tasalla ja vastaa sekä kansallisia että EU-tason vaatimuksia, jatkuva vaikutusarviointi ja säädösten mukauttaminen on syytä linjata osaksi kansallista lainsäädäntöprosessia. Vaikutukset tulee arvioida sekä uusien lakien valmisteluvaiheessa että voimaan tulleiden lakien seurannassa.

8.5.3 Puutteita C-Roads-määrittelyissä

Erilaisten viestintäteknologioiden (kuten lyhyen ja pitkän kantaman tiedonsiirtoratkaisut sekä hybridiympäristöt) integroiminen yhdeksi sujuvaksi ja GDPR-yhteensopivaksi järjestelmäksi edellyttää lisämäärityksiä eri viestien yksityisyyden suojaa koskevassa ohjeistuksessa ja lainsäädännössä. Koko C-ITS-järjestelmän yksityisyyden suojan kannalta EU:n luottamusmallin ulkopuolelle jäävien matkaviestinverkkoyhteyksien huomiointi kaipaa selkeyttämistä.

PKI-varmennus ja pseudonymisointi ovat käytössä, mutta varmenteiden dynaaminen vaihtaminen saattaa olla puutteellista. Tämä tarkoittaa, että pseudonyymit eivät välttämättä vaihdu riittävän usein, mikä voi johtaa käyttäjien jäljitettävyyteen pidemmällä aikavälillä. Varmenteiden viiden minuutin säilytysaikaa voi käytännössä olla vaikea valvoa. Lyhyen kantaman tiedonsiirtoratkaisussa voi kuka tahansa vastaanottaa salaamattomia ITS-G5-taajuusalueella lähetettyjä viestejä. Pitkän kantaman tiedonsiirrossa taas voi olla suurikin määrä viestien tilaamiseen pystyviä tai niihin muuten käsiksi pääseviä palveluntarjoajia. PKI-varmenteen täydentäminen edistynein kryptografisin menetelmin (esim. ryhmäallekirjoitus, Group Signature) voisi olla hyvä tekninen apu ehkäisemään turhaa henkilötiedon kertymistä.

Tietojen säilytysaikojen määrittely ja hallinta voi puuttua tai olla epämääräistä, mikä voi johtaa tarpeettomaan tietojen säilyttämiseen ja siten GDPR:n rikkomiseen. Säilytysaikojen selkeä määrittely auttaa rekisterinpitäjiä kehittämään toimintaansa ja noudattamaan GDPR:n vaatimuksia.

Edellä mainittujen puutteiden ratkaiseminen edellyttää C-Roads-yhteistoimielimiltä kehitystyötä, mutta myös jatkuvaa tarvetta arvioida teknologian ja säädösten kehitystä.

8.5.4 Yksityisyyden suoja on riskien ja saavutettujen hyötyjen tasapainottelua

C-ITS-palveluissa pyritään tasapainottamaan yksityisyyden suojaan liittyvät riskit ja saavutettavat hyödyt monilla mekanismeilla. C-ITS-viestit on suunniteltu suojaamaan henkilötietoja samalla, kun mahdollistetaan tehokas ajoneuvojen keskeinen sekä ajoneuvojen ja infrastruktuurin välinen viestintä.

Yksityisyyden suojaan liittyvät riskit liittyvät käyttäjän seurantaan ja paikkatiedon yhdistämiseen. C-ITS-viestien sisältämä sijaintitieto voi paljastaa tarkalleen, missä henkilö on ollut tietyllä hetkellä, mikä voi johtaa henkilökohtaiseen paikannukseen. Jatkuva sijaintitiedon kerääminen voi paljastaa liikkumismalleja, työpaikan tai kodin osoitteen sekä usein vieraillut paikat. Tällaisen tiedon käsittely voi johtaa ei-toivottuun valvontaan tai profilointiin. Erityisesti silloin, kun sijaintitieto yhdistetään muihin henkilötietoihin, se voi merkittävästi lisätä riskiä yksityisyyden suojan vaarantumiseen.

Pseudonymisoituja tunnisteita käytettäessä on riski, että riittävä lisätieto voi mahdollistaa käyttäjän tunnistamisen. On myös mahdollista, että henkilökohtaisia tietoja säilytetään pidempään puutteellisten käytäntöjen tai paikallisten lakien mukaisesti. Nämä voivat olla ristiriidassa yksityisyyden suojaa koskevien periaatteiden kanssa.

C-ITS-palveluiden avulla odotetaan saavutettavan monipuolisia hyötyjä. Liikenne on turvallisempaa, sujuvampaa ja päästöiltään pienempää. Se mahdollistaa teknologian kehittymisen, kun esim. automaattiset ajoneuvot kyetään paremmin integroimaan osaksi liikennejärjestelmää. C-ITS helpottaa rajat ylittävää yhteentoimivuutta kansainvälisessä liikenteessä ja kuljetuksissa.

C-ITS-järjestelmien mahdollistama turvallisuuden ja toimivuuden parantaminen oikeuttaa yksityisyyden suojaan liittyvien riskien hallitsemiseen siten, että henkilötietoja käsitellään huolellisesti säädösten vaatimien toimenpiteiden mukaan. Nämä toimenpiteet osoittavat, että C-ITS-palveluiden määrittelyissä on pyritty yksityisyyden suojan ja palveluiden toimivuuden väliseen tasapainoon, vaikka täydellinen anonymisointi ei ole mahdollista. Pyrkimys GDPR-vaatimusten mukaiseen henkilötietojen suojaamiseen on ollut selkeä, mutta tunnetut puutteet teknologiaan ja lainsäädäntöön liittyen sekä palveluiden toteutusta ja sääntelyä koskevan kokemuksen kertyminen edellyttävät jatkuvaa tilanteen tarkkailua.

9 Matkaviestinverkkoteknologian kyvykkyys ja mahdollisuudet

9.1 Tiedonsiirtoratkaisun vaikutus C-ITS-palveluiden toteuttamiseen

Pitkän kantaman tiedonsiirtoon perustuvat matkaviestinverkkopohjaiset ratkaisut ovat kehittyessään tarjonneet C-ITS-palveluiden toteuttamiseen kyvykkään vaihtoehdon lyhyen kantaman tiedonsiirtoon perustuville yleislähetysratkaisuille (broadcast). Traficomin teettämässä tutkimuksessa (Kilpiö et al. 2024) tunnistettiin matkaviestinverkkoteknologiaa puoltavina näkökulmina erityisesti seuraavat: kaupallisten matkaviestinverkkojen kattavuus on laaja, verkkoja ylläpidetään ja kehitetään ja niillä on riittävä C-ITS-palveluiden käyttöön soveltuva suorituskyky eli teknologian tarjoama kapasiteetti ja lyhyet viiveet. Voidaan nähdä, että ainakin näistä teknisistä syistä matkaviestinverkkotekniikkaan perustuvia ratkaisuja on ollut perusteltua alkaa kehittämään ja standardoimaan osaksi C-ITS-ratkaisuja (mahdolliset kaupalliset syyt jätetään tämän tarkastelun ulkopuolelle). Pitkän kantaman tiedonsiirtoratkaisuissa käytettävä Internet-verkon kiinteä osuus tarjoaa samankaltaisia ominaisuuksia kuin matkaviestinverkonkin osuus: laajaa kattavuutta, sisäänrakennettua ylläpitoa ja kehitystä sekä hyvää suorituskykyä.

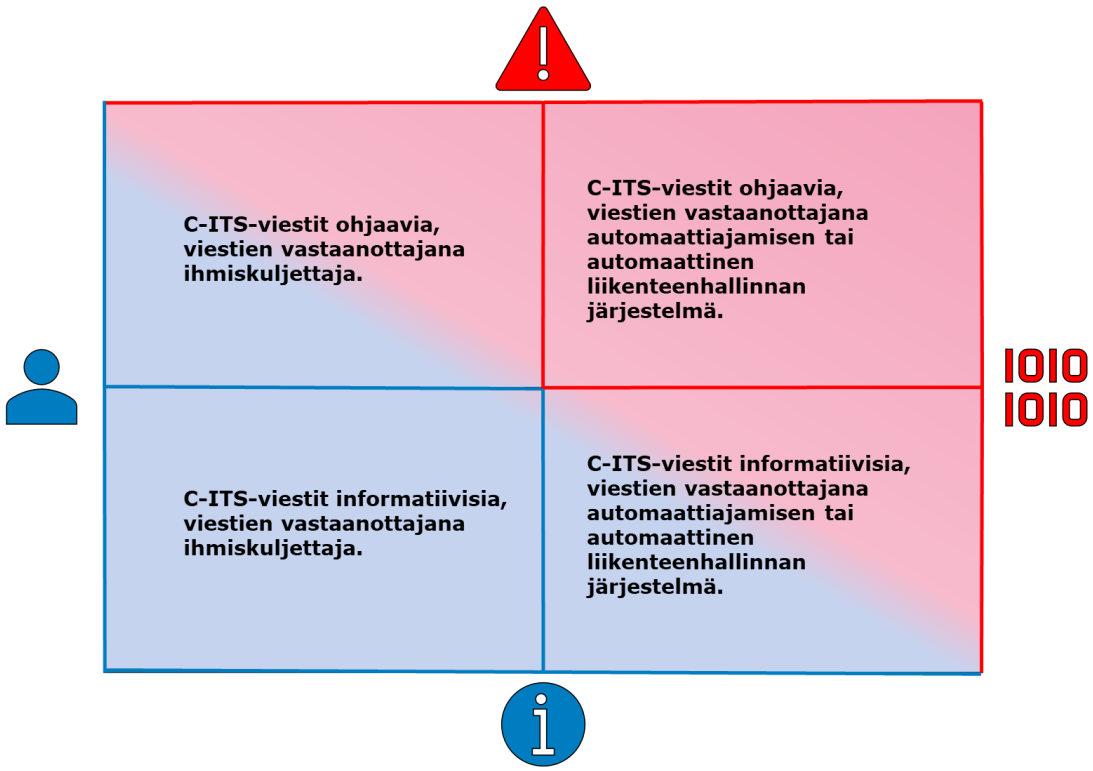
Toisessa Traficomin teettämässä tutkimuksessa C-ITS-palveluiden pilotoinnista (Kynsijärvi et al. 2024) todettiin, että kaupallisia matkaviestinverkkoja ja julkista Internet-verkkoa hyödyntävät pitkän kantaman tiedonsiirtoratkaisut toimivat tällä hetkellä verkkoalustan näkökulmasta ilman taattua verkon suorituskykyyn liittyvää palvelutasoa (ns. ”best-effort”-ympäristö). Kyseinen tutkimus myös suositteli, että tämän kaltaisissa verkkoympäristöissä voidaan (kyseisessä hankkeessakin suoritettujen suorituskykytestien mukaan) toteuttaa informatiivisia C-ITS-palveluita. Samalla tuotiin kuitenkin esille, että kun CCAM-toimialan (Cooperative Connected Automated Mobility) kehittyessä nykyisiä tai tulevia kehityksen alla olevia C-ITS-viestejä käytetään kriittisempiin liikenteenhallinnan tarkoituksiin tai niitä hyödynnetään jopa ajoneuvon ajokäyttäytymisen ohjaamisessa, olisi tärkeää pystyä tarjoamaan tälle viestinnälle ja keskeisille keskitetyille palveluille asianmukainen palvelutaso (Service Level Agreement, SLA).

Myös asiantuntijahaastatteluissa (Swarco haastattelu 2024) nostettiin esiin vastaava jaottelu turvallisuuskriittisiin sekä liikenteen tehokkuutta ja mukavuutta parantaviin C-ITS-palveluiden sovelluskohteisiin. Pitkän kantaman tiedonsiirrossa matkaviestinverkkojen käyttöä pidettiin haastavana turvallisuuskriittisissä sovelluksissa. Haastattelussa tuli myös esille verkon toiminnan laatuun liittyvä palvelutasolupauksen (SLA) puute sekä puutteelliset verkon komponentteihin liittyvät määrittelyt.

Edellä mainittujen näkökulmien takia C-ITS-palveluita voisi olla perusteltua tarkastella kahdella eri asteikolla; mikä taho viestejä hyödyntää (ihmiskuljettaja vai dynaamisista ajotehtävistä vastaava automaattiajon tai automaattisen liikenteenhallinnan järjestelmä) sekä millaisia viestit ovat luonteeltaan (informoivia vai ohjaavia), kuvan 17 mukaisesti.

Edellä esitetyn mukainen yhteistoiminnalliseen ajamiseen tähtäävä V2X-palveluiden (joiksi myös C-ITS-palvelut voidaan laskea) käyttötapaus on tunnistettu CAR 2 CAR Communication -konsortiossa potentiaalisena tulevaisuuden käyttötapauksena. Tällöin ajoneuvot voivat jakaa tietoa aikeistaan toisillensa, jolloin

esimerkiksi automaattiajoneuvojen toiminnan yhteensovittaminen eri liikennetilanteissa helpottuu (CAR 2 CAR Communication Consortium, 2019). Kytkös C-ITS- ja CCAM-kehityksen välillä on tunnistettu myös CCAM-kumppanuusohjelmassa (CCAM Partnership, 2023), jossa julkisen ja yksityisen sektorin toimijat pyrkivät yhtenäistämään tutkimus- ja kehityspanoksiaan CCAM-teknologioiden ja -palveluiden käyttöönoton kiihdyttämiseksi Euroopan laajuisesti. Kumppanuusohjelmaa ohjaa strateginen tutkimus- ja innovaatioagenda (Strategic Research and Innovation Agenda, SRIA), joka on useammalle vuodelle jakautuva tiekartta. Tässä tiekartassa C-ITS-kehitys tunnistetaan tärkeänä tukitoimintona CCAM-kehityksessä tarvittavan digitaalisen infrastruktuurin rakentamiseksi. Tiekartassa tunnistetaan C-ITS-viestien informatiivisen käyttötapauksen lisäksi myös viestien ohjaava vaikutus ajoneuvoille esimerkiksi ohitus- tai risteystilanteissa (CCAM Partnership, 2023).



Kuva 17. C-ITS-palveluiden luokittelu

Kuvan 17 mukaisesti ensimmäisessä kategoriassa (vasen ylänurkka) C-ITS-viestit ovat ohjaavia ja viestien vastaanottajana on ihmiskuljettaja. Tässä tilanteessa C-ITS-viestit tarjoavat liikenteen ohjaukseen liittyvää tietoa (esimerkiksi rajoitus- tai liikennevalojen tilatietoja), jota kuljettajan tulee noudattaa. C-ITS-viestien välittämä tieto rinnastuu muiden liikennemerkkien sekä liikenteenohjauslaitteiden välttämiin tietoihin. C-ITS-viestien oikea-aikaisuus ja luotettavuus korostuvat.

Toisessa kategoriassa (vasen alanurkka) C-ITS-viestit ovat informatiivisia, ja viestien vastaanottajana on ihmiskuljettaja. Tällöin C-ITS-viestit tarjoavat tietoa liikenneympäristöstä ja -tilanteesta, jotta kuljettaja voi suhteuttaa esimerkiksi ajonopeutensa tai reittivalintansa sopivaksi. C-ITS-viestit voivat varoittaa myös yllättävästä tai aikakriittisestä tilanteesta (esimerkiksi moottoritielle hajonnut ajoneuvo tai punaisia liikennevaloja päin liikkuva ajoneuvo), joka vaatii kuljettajalta välitöntä reagointia. Viestiin reagoimatta jättäminen saattaa lisätä onnettomuuden todennäköisyyttä tai lisätä onnettomuuden vakavuutta. C-ITS-viestien oikea-

aikaisuus ja luotettavuus korostuvat, välityksen viive muodostuu merkittäväksi tekijäksi yllättävistä ja lähellä olevista aikakriittisistä tilanteista varoitettaessa.

Kolmannessa kategoriassa (oikea ylänurkka) C-ITS-viestit ovat myös ohjaavia, mutta viestien vastaanottajana on automaattiajamisen tai automaattisen liikenteenhallinnan järjestelmä. Vaikka ajoneuvot havainnoivat ympäristöään myös omien sensoreidensa avulla ja kahdentavat toimintoja, niin C-ITS-viestien välittämä ohjaus vaikuttaa ajoneuvojen ajokäyttäytymiseen. Tällainen tilanne voisi olla esimerkiksi edellä mainitun CAR 2 CAR Communication -konsortion esittämä tulevaisuuden käyttötapaus yhteistoiminnallisesta ajamisesta (esimerkiksi tielle liittyminen tai risteysalueella toimiminen). Tällaiset käyttötapaukset ovat pidemmällä tiekartalla ja esimerkiksi erityisesti vastuukysymysten kannalta ratkaistavia asioita on paljon. Automaattisen liikenteenhallinnan järjestelmä puolestaan suorittaa liikenteenhallinnallisia toimenpiteitä, kuten joukkoliikenne-etuuksien toteuttamista tai liikennevalojen ohjausta, suoraan C-ITS-viestien välittämään tietoon pohjaten (esimerkiksi ajoneuvojen välittämät CAM-viestit). C-ITS-viestien laatu, luotettavuus ja viive ovat kriittisiä turvallisen toiminnan varmistamiseksi.

Neljännessä kategoriassa (oikea alanurkka) C-ITS-viestit ovat informatiivisia ja viestien vastaanottajana on automaattiajamisen tai automaattisen liikenteenhallinnan järjestelmä. C-ITS-viestit tarjoavat ajoneuvoille laajennetun digitaalisen horisontin, jolloin ne saavat tietoa omien sensoreiden kantomatkan ulkopuolelta. Ajoneuvo käyttää näitä tietoja omien tietojensa kahdentamiseen (rinnakkainen varajärjestelmä ajoneuvon sensoreiden keräämän tiedon varmentamiseksi), mutta niitä ei käytetä yksinomaisena toiminnan perusteena. Vastaavasti C-ITS-viestien välittämiä tietoja hyödynnetään automaattisessa liikenteenhallinnan järjestelmässä, mutta kriittisissä päätöksissä esimerkiksi liikennepäivystäjä voi tehdä lopullisen päätöksen tarvittavista toimista.

Vaikka tämä selvitystyö ei ota kantaa tiedonsiirtoteknologioiden soveltuvuuteen eri C-ITS-palveluiden toteuttamiseksi (työn rajausten mukaisesti, katso luku 1.2), niin edellä hahmoteltu kategorisointi antaa aihetta kuitenkin jatkossa pohtia tätä näkökulmaa. Yllä kuvattua aihetta käsitellään seuraavissa alaluvussa C-ITS-palveluiden toteuttamiseen liittyvän verkkoteknisen kehityksen ja yleisen verkkoarkkitehtuurisen suunnittelun näkökulmasta. Näkökulmat perustuvat selvitystyöryhmän asiantuntemukseen tietoliikenneverkkoteknologioiden hyödyntämisestä laajoissa WAN-verkkoratkaisuissa (Wide Area Network) sekä osana IoT-ratkaisuja (Internet of Things).

9.2 Lyhyen ja pitkän kantaman tiedonsiirtoratkaisujen erot

C-ITS-palveluiden kehityksestä on hyvä huomata, että hyvin pitkään C-ITS-palveluita kehitettiin lyhyen kantaman ratkaisuihin sekä radiotekniikan käyttöön perustuen, ja tämän taustan vaikutukset näkyvät tällä hetkellä monessa asiassa. Lyhyen kantaman ratkaisuihin perustuva toimintaympäristö eroaa tietoliikennetekniisesti merkittävästi pitkän kantaman toimintaympäristöstä.

Lyhyen kantaman tiedonsiirron radioteknisessä toteutuksessa käytössä oleva tietoliikennekapasiteetti on täysin tiettyyn käyttötarkoitukseen varattu. Tarjolla oleva C-ITS-yksiköiden käyttämä radiokanavan kapasiteetti on täysin C-ITS-palveluiden käytössä, eikä kilpailijoita tästä tiedonsiirtokapasiteetista ole. Tämäkään toteutusmalli ei toisaalta takaa tiettyä palvelutasoa. Radiokanavan kuormittuessa

pakettien välityksessä saattaa esiintyä viiveitä ja pahimmillaan viestin välitys voi epäonnistua.

Tietoturvallisuuden näkökulmasta radioteknologia on lähtökohdiltaan erittäin avoin. Tienvarsiyksiköt viestivät ympäristölleen majakan tavoin (broadcast) ja kaikki, jotka haluavat ”virittää vastaanottimensa” samalle taajuudelle, voivat kuunnella. Kuuntelemisen lisäksi mikä tahansa taho voi käytännössä myös lähettää viestejä sopivalla laitteistolla ja ohjelmointiosaamisella. Tämän kaltaisessa ympäristössä C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) tuottaa ratkaisulle erinomaisen tietoturvan. Se pitää huolen, että viestien vastaanottajat pystyvät varmistamaan, että viesti on lähetetty luotetulta taholta (autentikointi), ja tarkastamaan jokaisen vastaanotetun paketin osalta, että viestiä ei ole manipuloitu matkalla (eheys). Hallinnolliselta kannalta lyhyen kantaman tiedonsiirtoympäristön toteuttaminen on haastavaa erityisesti katuverkolla, jonka ylläpidosta vastuussa ovat kunnat. C-ITS-tienvarsiyksiköiden verkon peiton toteuttaminen teiden ja katujen varsille on merkittävä investointi puhumattakaan kyseisten laitteiden ylläpitotoiminnan kustannuksista ja elinkaaren hallinnasta (mm. ylläpidon kenttähuollon palvelu- ja reagointiajat, hajautetut varaosavarastot, ohjelmistojen päivitykset sekä laitevaihtotarpeet teknologiakehityksen osana).

Pitkän kantaman tiedonsiirtovaihtoehto on verkon näkökulmasta monelta osin päinvastainen; verkossa välitettävien palveluiden suhteen suljetun sijaan täysin avoin. Pitkän kantaman tiedonsiirrossa käytetään avointa kuluttajille suunnattua matkaviestinverkkoa, josta siirrytään kiinteän verkon puolelle käyttäen avointa Internet-verkkoa. Verkon tarjoamasta kapasiteetista kilpailee lukematon määrä kuluttajien sekä yritysten käyttämiä sovelluksia, ja viestin polku ajoneuvo- tai tienvarsiyksiköltä C-ITS-keskusyksikölle (esim. EU-alueella Microsoftin Azure -konesalissa sijaitseva pilvipalvelu) saattaa kulkea useiden kymmenien tai jopa satojen verkkolaitteiden läpi, joista mikään ei ole C-ITS-järjestelmän omistajan hallinnassa. Tällä tavalla käytettynä julkinen verkko tai verkot eivät siis tarjoa C-ITS-palveluille kapasiteetin tai viiveiden osalta minkäänlaista palvelutasolupausta.

Pitkän kantaman tiedonsiirtoon perustuvien C-ITS-ratkaisujen tietoturvallisuuden kannalta nykyinen C-ITS-turvatunnusten hallintajärjestelmä (EU CCMS) on sovellettavissa julkisen verkon toimintaympäristöön. Järjestelmä tarjoaa siinäkin ympäristössä hyödyllisiä tiedon turvallisuuteen liittyviä ominaisuuksia. Toisaalta tämäkin tekninen toteutus osoittaa hyvin lyhyen ja pitkän kantaman tiedonsiirtoon perustuvien ratkaisujen kehittämisen eri lähtökohdat. Se, mikä lyhyen kantaman tiedonsiirtoratkaisussa on hyvin perusteltua, voi pitkän kantaman tiedonsiirrossa olla jopa tarpeetonta tai ainakin ratkaistavissa toisella tavalla. Avoin IP-protokollaan perustuva Internet-verkko tarjoaa samojen asioiden (luotettava käyttäjien autentikointi ja tiedon salaus) hoitamiseksi useita valmiita ja kevyempiä ratkaisuja. Näitä samoja julkisista verkoista tuttuja tietoturvallisuusratkaisuja (TLS ja X.509) käytetään myös C-Roads-spesifikaatioiden vaatimusten mukaisesti pitkän kantaman tiedonsiirtoratkaisuissa C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) tarjoamien ratkaisujen lisäksi.

Laajamittaisesti käyttöönotettavan lyhyen kantaman tiedonsiirtoon perustuvan C-ITS-ratkaisun ongelmat liittyvät erityisesti korkeisiin rakentamis-, huolto ja ylläpitokustannuksiin. Se on myös laiterikoille herkkä. Yksittäisen tienvarsilaitteen rikkoutuminen estää alueellisesti ajoneuvojen ja infran välisen viestinnän (laitteiden kahdennuksella voidaan toki tätä parantaa). Käytetty radiotaajuus on herkkä

lähettäjän ja vastaanottajan välissä oleville fyysisille esteille (”line-of-sight” -vaatimus). Pitkän kantaman tiedonsiirtoon perustuva ratkaisu on kaikkien yllä esitettyjen lyhyen kantaman ratkaisun heikkouksien osalta vahvempi ratkaisu. Verkolla on valmis laaja kattavuus sekä ammattimainen verkon kehitys ja ylläpito. Solujen koko ja todennäköisyys taajuus- tai tukiasematason peiton päällekkäisyyteen on suuri, eivätkä käytettävät taajuudet ole niin herkkiä fyysisille esteille. Verkkoteknisen suorituskyvyn kannalta molemmat ratkaisut ovat vahvoja. Lyhyen kantaman ratkaisu ei tarjoa yhtä paljon tietoliikennekapasiteettia kuin esimerkiksi 5G-verkot, mutta C-ITS-palveluiden tarpeisiin kapasiteetti on riittävä ja se on täysin niiden käyttöön varattu.

9.3 Pitkän kantaman tiedonsiirtoratkaisussa tunnistettuja ongelmia

Julkisten matkaviestinverkkojen ja Internet-verkon suorituskykyyn liittyen on tehty testejä, jotka ovat tuottaneet lupaavia tuloksia verkon hyödyntämiseen liittyen (Kynsijärvi et al. 2024). Ongelmaksi näissä muodostuu testien pistemäisyys ja kesto. Testien perusteella voidaan todeta, että kyseiset verkot tarjoavat pääasiassa riittävän, jopa erinomaisen suorituskyvyn C-ITS-palveluiden toteutukselle. Matkaviestinverkkojen suorituskykyä on laajamittaisesti hankala testata, sillä matkaviestinverkon suorituskyky voi vaihdella merkittävästi eri maantieteellisillä alueilla, jopa yhden kaupungin sisällä, ja erityisesti verkkojen kunto ja suorituskyky vaihtelevat paljon eri maiden välillä. Testit eivät myöskään ole sisältäneet kovin laajojen käyttäjämäärien kokeiluja (joskin näistä on kokemusta mm. Hollannin C-ITS-ekosysteemistä). Toisaalta laajakaan verkon kattavuus ei ole täydellinen, joten verkon peitossa voi olla joskus aukkoja C-ITS-järjestelmien toiminnan kannalta kiusallisissakin kohdissa.

Ongelmallisia matkaviestinverkon suorituskykyyn vaikuttavia tekijöitä voivat olla erilaiset ulkoiset tekijät, kuten merkittäviä käyttäjämääräpiikkejä aiheuttavat massatapahtumat, liikenneruuhkat, liikenneonnettomuustilanteet tai operaattorin runkoverkon ongelmat. Internet-verkon kiinteä osuus on altis kyberhyökkäystilanteille (esim. alueelliset tai palvelukohtaiset palvelunestohyökkäykset), verkko-operaattoreiden runkoverkossa tapahtuville laiterikoille ja kaapelikatkoksille tai globaalien keskeisten runkokaapelien rikoille. Erityisenä ongelmana on syytä nostaa Internet-verkossa sijaitsevien palveluiden alttius kyberturvallisuuteen liittyville ongelmille. Näistä keskeisenä palvelunestohyökkäykset (Distributed Denial of Services, DDOS), jotka ovat erityinen riski palveluille, joilla on julkisia palvelurajapintoja avoimessa verkossa (julkiseen verkkoon kiinni liitetyt pilvipalvelut tai konesaleihin sijoitetut palvelut).

Yllä kuvattuja julkisen verkon ongelmia voidaan pitää hyvin perustavanlaatuisina erityisesti tosiaikaisten ja jatkossa turvallisuuskriittisten C-ITS-palveluiden toteutukseen liittyen. C-ITS-ratkaisuiden kehittämisessä on panostettu merkittävästi osapuolten luottamuksellisuuden ja C-ITS-viestien eheyden varmistamiseen (EU CCMS). Pitkän kantaman ratkaisussa merkittävää kehitystä on tehty myös taustajärjestelmien välisten istuntojen salaamiseksi ja osapuolten autentikointiin (C-Roads). Pitkän kantaman ratkaisuissa verkkoihin liitettyjen palveluiden sekä niiden hyödyntämien verkkoratkaisujen suojauksen (esim. suljetut WAN-verkkoratkaisut) ja palvelutason (SLA) kehittämiseen ei ole kuitenkaan juurikaan kiinnitetty huomiota.

On hyvin todennäköistä, että jo pelkästään NIS2-direktiivi tulee luomaan merkittäviä lisävaatimuksia Euroopan laajuisen C-ITS-järjestelmän kehittämiselle. Vaatimukset kohdistuvat nimenomaan C-ITS-palvelutoteutusten hyödyntämien verkkototeutusten suunnitteluun ja toteutukseen, sillä liikenneala on yksi NIS2-direktiivin määrittelemistä erittäin kriittisistä soveltamisaloista. Tämä määritelmä asettaa liikennealalla käytettäville teknisten järjestelmien hallinnalle ja niiden toteutusten tietoturvallisuudelle omia vaatimuksia.

9.4 Kehityssuuntia

Huolimatta edellä esille nostetuista pitkän kantaman tiedonsiirtoratkaisujen tietoliikennearkkitehtuureihin liittyvistä ongelmista, on tietojärjestelmäarkkitehtuuria monelta osin myös helppo kehittää.

Matkaviestinverkon osuus toiminnassa on tällä hetkellä hieman hankalampi. Matkaviestinverkosta voi ostaa organisaatiokohtaisia yksityisiä APN-palveluita (private Access Point Name), mutta nämä ovat aina operaattorikohtaisia, eivätkä verkot tällä hetkellä tarjoa sovelluskohtaisia QoS- tai CoS-palveluita (Quality/Class of Service), jotka voisivat tarjota valikoidulle palvelulle parempaa palvelutasoa. Erilaisia tulevaisuuden mahdollisia kehitysehdotuksia matkaviestinverkon palvelutason parantamiseksi, mm. verkon viipalointi, on esitetty tarkemmin Traficomin aiemmissa tutkimuksissa (Kilpiö et al. 2024).

Kansallisesti matkaviestinverkko rakentuu pitkälti nykyisellään ja etenkin lähitulevaisuudessa 4G- ja 5G-verkkoteknologioiden varaan, sillä 5G-verkkoteknologian käyttöönotto on edennyt nopeasti Euroopassa viime vuosina. Euroopan komissio on toimillaan pyrkinyt edistämään 5G-verkkoteknologian käyttöönottoa sekä varmistamaan kehityksen tarvitseman rahoituksen. Komissio hyväksyi vuonna 2016 5G-toimintasuunnitelman, jonka tavoitteena oli verkkoteknologian varhainen käyttöönotto kaikkialla Euroopassa (EU 2016/588, 2016). Toimintasuunnitelma listasi mm. vuoden 2020 tavoitteeksi 5G:n käyttöönoton aloittamisen kaikissa jäsenvaltioissa sekä keskeytymättömän kattavuuden varmistamisen vuoteen 2025 mennessä keskeisillä kaupunkialueilla ja tärkeimpien liikenneväylien varrella. Lisäksi komissio täydensi 5G-tavoitteita vuonna 2021 julkaistussa Euroopan digitaalinen kompassi -dokumentissa asettamalla lisätavoitteen, jonka mukaan 5G-yhteyksien tulee vuoteen 2030 mennessä kattaa kaikki asutut alueet (EU 2021/118, 2021). Komissio on myös rahoittanut 5G-kehittämishankkeita keskeisillä liikennekäytävillä Verkkojen Eurooppa -rahoitusvälineen digitalisaatio-osion (CEF Digital) avulla. Rahoitusta on myönnetty niin varsinaisen aktiivi- ja passiivi-infrastruktuurin kehittämiseen kuin tutkimushankkeisiin (Euroopan komissio, 2022). Euroopan komissio panostaa myös tulevan 6G-verkkoteknologian kehitykseen ja tutkimukseen, ja 6G:n suhteen odotetaan standardointitoimien alkavan vuoden 2025 kuluessa. Näitä toimia varten Euroopassa on perustettu vuonna 2021 Smart Networks and Services Joint Undertaking (SNS JU) -yhteistyötoimielin (De Luca 2024).

Viidennen ja kuudennen sukupolven langattomien verkkoteknologioiden hyötyjä ovat mm. kasvava tiedonsiirtonopeus, alhainen latenssi sekä korkea luotettavuus. Nämä kaikki ovat ominaisuuksia, jotka hyödyttävät myös C-ITS-palveluiden toteutuksessa. Aiemmassa Traficomin selvityksessä (Kilpiö et al. 2024) tunnistettiin KPI-mittareita matkaviestinverkon kautta toimivien C-ITS-palveluiden palvelutasolle. Näitä ovat käytettävyys (verkon peitto), luotettavuus (verkon pakettihävikki) ja eheys (lataus-/lähetysnopeus ja latenssi). Samassa tutkimuksessa

todettiin, että verkkoteknologisen suorituskyvyn kannalta jo käytössä olevat 4G-verkot mahdollistavat C-ITS-palveluiden toteutuksen. Verkkoteknologian lisäksi matkaviestinverkon järjestelmän kapasiteettiin vaikuttavat olennaisesti myös eri alueilla käytetty verkon spektri ja verkkotopologia. Eri taajuusalueet sopivat eri käyttötarkoituksiin, ja pienemmän radiosignaalin vaimenemisen vuoksi matalilla taajuuksilla sijaitsevilla kapeammilla kaistoilla saavutetaan suurempi kattavuus mutta pienempi kapasiteetti. Korkeammilla taajuuksilla sijaitsevilla leveämmillä taajuusalueilla puolestaan saavutetaan korkea kapasiteetti, mutta se vaatii myös tiheämpää tukiasemaverkostoa. Selvityksessä nostettiin esiin myös luvun 9.3 keskeinen kritiikki; matkaviestinverkot ovat luonnostaan hyvin riippuvaisia ympäristöstä, ja heikkoja palvelutasoja esiintyy kaikilla kotimaisilla operaattoreilla riippuen niiden paikallisen verkon käyttöönotosta ja verkkostrategiasta. Eli keskeiseksi ongelmaksi muodostuu taatun palvelutason puute erityisesti turvallisuuskriittisten C-ITS-palveluiden suhteen. Kehittyvät ja tulevaisuuden verkkoteknologiat tuovat kuitenkin edistyneempiä mekanismeja ja uusia ominaisuuksia palvelutason parantamiseksi, mutta verkkoteknologioiden kehitys itsessään ei takaa tiettyjä palvelutasoja C-ITS-palveluille.

Voidaan kuitenkin olettaa, että tulevaisuuden verkkoteknologioiden kehitys ja uudet ominaisuudet tukevat myös C-ITS-palveluiden toteuttamista pitkän kantaman tiedonsiirtotavoilla. Vaikutusten suuruusluokkaa on hankala tarkasti arvioida, sillä 6G-verkkoteknologia on edelleen tutkimus- ja kehitysvaiheessa, joten sen todellinen suorituskyky on siis osittain spekulatiivista. Myöskään 5G-verkkoteknologialla ei ole vielä saavutettu tarvittua kattavuutta (esimerkiksi suurten kaupunkien ja keskeisten liikenneväylien ulkopuolella), ja tämänkin verkkoteknologian suhteen tapahtuu edelleen uutta kehitystä, innovaatiota ja uusia standardien julkaisuja. Muun muassa tietoliikenneverkkoratkaisuja ja -teknologioita tarjoavat yritykset, kuten Nokia, ovat visioineet etenkin 6G:lle lukuisia uusia käyttötapauksia mahdollistaen laajamittaiset digitaaliset kaksoset ja lisätyn todellisuuden sovellutukset fyysisen maailman jatkeeksi (Viswanathan & Mogensen, 2023). Ajatellen CCAM-sovellutuksia ja liikenteen kehittymistä tulevaisuuden verkkoteknologiat todennäköisesti mahdollistavat myös huomattavan määrän uusia liikenteen käyttötapauksia, joita ei välttämättä lyhyen kantaman tiedonsiirtoratkaisun varaan kyettäisi rakentamaan sen kapasiteetin rajallisuuden takia. Voidaan olettaa, että tulevaisuudessa matkaviestinverkot ovat entistä keskeisempiä myös liikennesektorin näkökulmasta. Joka tapauksessa C-ITS-palveluiden käyttöönoton näkökulmasta ei ole tarpeen jäädä odottamaan verkkoteknologioiden kehittymistä, vaan esimerkiksi nykyisillä 4G- ja 5G-verkkoteknologioilla voidaan kattaa suuri osa C-ITS-palveluista, mikäli ajoittaiset alueelliset vaihtelut sekä hetkittäiset alentumiset palvelutasossa hyväksytään. Tämä voi vaatia tarkemman C-ITS-palvelukohtaisen tarkastelun luvun 9.1 ehdotusten mukaisesti.

Kiinteän Internet-verkon osalta on tarjolla paljon kehitystoimenpiteitä. C-ITS-järjestelmän C-ITS-keskusyksiköiden sijaintia voidaan säännellä (esim. vain kotimaisiin konesaleihin), ja C-ITS-keskusyksiköiden välinen tietoliikennetoteutus voidaan toteuttaa erikseen kilpailutettavalla suljetulla verkkoratkaisulla, joka antaa yhteyksien palvelunlaadulle takuun. Jos C-ITS-keskusyksiköiden sijaintipaikkana käytetään keskeisiä globaaleja pilvipalveluita, niin näihinkin pystytään erikseen ostamaan suljettuja tietoturvallisia SLA:lla varustettuja tietoliikenneyhteyksiä. EU-tasolla voitaisiin toteuttaa maiden välisten tiedonvaihtopalvelimien välisten yhteyksien muodostamiseksi suljettu verkkoympäristö, johon kunkin maan tai organisaation tiedonvaihtopalvelimet velvoitetaan liittymään Euroopan laajuiseen C-

ITS-luottamusverkkoon pääsemiseksi. Tämä tarjoaisi tiedonvaihtopalvelimien välisille yhteyksille taatun palvelutason (kapasiteetti) ja palvelut voitaisiin näin eristää myös julkisesta verkosta, jolloin niihin ei voisi kohdistaa palvelunestohyökkäyksiä. Samankaltainen järjestely voitaisiin toteuttaa myös kansallisesti C-ITS-keskusyksiköiden osalta, jolloin niiden väliseen viestintään voitaisiin tarjota palvelutaso ja viestintä olisi suljettua.

10 Kansallinen tahtotila C-ITS-palveluiden toteuttamiseksi

Mikään EU- tai kansallinen sääntely ei velvoita jäsenvaltioita toteuttamaan C-ITS-palveluita tai ottamaan käyttöön niihin liittyviä komponentteja, kuten keskusyksiköitä. Uudistettu ITS-direktiivi (EU 2023/2661, 2023) ja sen alaiset delegoidut asetukset tuovat kuitenkin tiettyjä velvoitteita, ja niissä pidemmän tähtäimen pyrkimyksenä on ITS-palveluiden laajamittainen käyttöönotto jäsenvaltioissa.

Uudistetun ITS-direktiivin tavoitteena on ollut päivittää ja laajentaa direktiivin soveltamisalaa kattamaan uusia palveluita ja teknologioita, mukaan lukien C-ITS-palvelut. Osa niistä määrittelyistä, jotka vuoden 2019 delegoidussa asetuksessa C-ITS-palveluiden käyttöönotosta (EU C/2019/1789, 2019) oli mainittu, on näin ollen huomioitu direktiivin uudistuksessa, vaikka se ei suora uudelleentarkastelu vuoden 2019 hylätystä delegoidusta asetuksesta olekaan. Uudistetussa ITS-direktiivissä otetaan siis selvästi vahvempi kanta ja todetaan C-ITS-palveluiden olevan yksi ITS-palveluiden luokka, jolloin voidaan päätellä, että C-ITS-palveluiden sääntely ja edistäminen ovat edelleen aktiivisesti esillä EU-tasolla sekä komission agendalla.

Tätä päätelmää tukee myös Euroopan komission täytäntöönpanopäätös direktiivin 2010/40/EU työohjelman vahvistamisesta vuosiksi 2024–2028 (C/2024/6798, 2024), jossa myös C-ITS on omana toimenaan huomioitu. Tähän toimeen liittyvät C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS), yhdenmukaistettuja C-ITS-palveluita sekä C-ITS-palveluiden kehittämistä ja toteuttamista koskevat määritykset. Edellä luetelluista määrityksistä C-ITS-turvatunnusten hallintajärjestelmää koskevat määritykset ovat jo julkaistu ja ne ovat myös keskeinen osa tätä selvitystyötä. Työohjelmassa todetaan että, ”yhteiset määritykset voitaisiin toteuttaa uutena delegoituna säädöksenä tai voimassa olevan delegoidun säädöksen muutoksena”. Käytännössä tämä voi siis johtaa siihen että, työohjelman toimikauden puitteissa aloitetaan uuden C-ITS:n täytäntöönpanoa koskevan delegoidun asetuksen valmistelu.

Kansallista tahtotilaa liikenteen digitalisaation ja automaation edistämiseksi on kuvattu keskeisimmissä hallinnonalan julkaisuissa, vaikka näissä ei juurikaan mainintoja C-ITS-järjestelmän käyttöönotosta varsinaisesti ole. C-ITS-kehityksen voidaan kuitenkin katsoa kuuluvan osaksi ja olevan yksi keskeinen toimi liikenteen digitalisaation edistämiseksi. Tästä näkökulmasta myös C-ITS-kehitystä tukevia kirjauksia voidaan katsoa olevan useita.

Ainut hallinnonalan julkaisu, joka varsinaisesti mainitsee C-ITS-palvelut, on Liikenteen automaation lainsäädäntö- ja avaintoimenpidesuunnitelma (Miettinen et al. 2021). Tässä julkaisussa C-ITS-toteutusta käsitellään tiedon hyödyntämisen ja tieliikenteen automaation tarvitseman tiedonjakoinfrastruktuurin näkökulmasta. Dokumentissa tunnistetaan C-ITS-viestien välittämät tiedot oleellisiksi liikenteen automaation edistämiseksi.

Pääministeri Petteri Orpon hallitusohjelmassa (Valtioneuvosto 2023) on oma luku liikenteen palveluiden uudistamiselle digitalisaatiota hyödyntäen. Tässä yhteydessä mainitaan toimina, joita hallitus edistää, mm. liikenne- ja logistiikka-alan digitalisaatio ja automatisaatio, uudenlaisten liiketoimintamallien syntyminen ja hyödyntäminen sekä liikennejärjestelmän tehokkuus.

Valtioneuvoston periaatepäätöksessä liikenteen automaation edistämiseksi (LVM/2021/137) on myös huomioitu liikenteen verkottuminen ja tiedonvaihtotarpeet, ja siinä on tehty linjaus liikenteeseen liittyvän tiedon vaihtamisen merkittävästä tehostamisesta huomioiden erityisesti matkaviestinverkkoteknologian kehitys ja Suomen edelläkävijyys tällä rintamalla.

Liikenne- ja viestintäministeriön hallinnonalan konsernistrategia (Liikenne- ja viestintäministeriö 2024) on puolestaan asettanut hallinnonalalle useita digitalisaatioon ja dataan liittyviä tavoitteita. Erityisesti dataan perustuvia liikenteen palveluita koskevaa tavoitetta voidaan katsoa edistettävän C-ITS-kehityksen avulla. Yksi keskeinen ajuri C-ITS-kehitykselle on liikenneturvallisuuden parantaminen.

Liikenneturvallisuusstrategia 2022–2026 (Rekola et al. 2022) tunnistaa myös teknologisen kehityksen liikenneturvallisuutta lisäävänä kehityskulkuna. Strategian yhtenä toimenpiteenä edistetään toimintamallia, jossa ajoneuvojen ja infrastruktuurin tuottamaa dataa voidaan hyödyntää reaaliaikaisen ja ennakoivan olosuhdetilannekuvan muodostamisessa sää- ja kelitietojen osalta. Tällaisella infrastruktuurin ja ajoneuvojen yhteen kytkennällä ja informaation jakamisella odotetaan saavutettavan useita liikenneturvallisuushyötyjä. C-ITS on yksi konkreettinen tapa edellä mainittuihin toimiin.

Tämän raportin kirjoittamisen aikaan lausuntokierroksella ollut Liikenne 12 -suunnitelmaluonnos vuosille 2026–2037 valtakunnallisen liikennejärjestelmäsuunnitelman päivittämiseksi (Valtioneuvosto 2024) käsittelee omassa luvussa liikenteen digitaalisen toimintaympäristön kehittämistä. Tässä yhteydessä keskeiseksi toimeksi tunnistetaan kansallisten toimintamallien kehittäminen siten, että ne tukevat liikennejärjestelmää koskevan tiedon tuottamista, jakamista ja hyödyntämistä kustannustehokkaasti ja lisäarvoa tuottavalla tavalla. Myös viestintäyhteyksien kehittäminen (kattavat matkaviestinverkot) on tunnistettu edellytyksenä liikenteen digitalisaatiolle.

C-ITS-palveluiden toteutus on yksi konkreettinen keino viedä eteenpäin näitä edellä mainittuja ylätason strategisia tavoitteita. Dokumenteista ilmenevä vahva kytkös liikenteen digitalisaation ja viestintäyhteyksien välillä voidaan katsoa tukevan C-ITS-toteutuksen näkökulmasta nimenomaan pitkän kantaman tiedonsiirtoratkaisuun pohjautuvaa toteutusmallia.

Kansallisten näkemysten tarkemmassa kartoittamisessa tukeuduttiin työn aikana lisäksi asiantuntijatyöpajaan, jossa oli edustettuna keskeisimmät kansalliset hallinnonalan toimijat sekä kuntasektorin edustajia. Suomessa julkiset toimijat ovat pitkälti vastuussa tie- ja katuverkon ylläpidosta, kehittämisestä sekä liikennetiedottamisesta, joten myös C-ITS-palveluiden järjestämisessä on näillä toimijoilla luontainen rooli. Asiantuntijatyöpajassa esitetyt näkemykset olivat asiantuntijoiden henkilökohtaisia näkemyksiä, eivätkä siten vastaa välttämättä hallinnonalan toimijoiden ja virastojen virallista kantaa. Osallistujat ovat kuitenkin C-ITS-toteutuksen kannalta keskeisissä rooleissa näissä organisaatioissa, joten heidän näkemyksensä kuvaavat kohtuullisen hyvin kansallista tahtotilaa yleisellä tasolla.

Asiantuntijatyöpajan tulosten perusteella käsitys C-ITS-palveluiden tuomista hyödyistä sekä toteutuksen aikataulusta ovat osittain epäselviä. Tämä korostui erityisesti pitkän kantaman tiedonsiirtoratkaisun osalta. Toisaalta sääntelyn odotetaan luovan luottamukseen perustuvan yhteistyöympäristön, joka tukee C-ITS-palveluiden kehittymistä. C-ITS-palveluiden käyttöönotossa suositaan vaiheittaista

etenemistä, mikä mahdollistaa toimintojen asteittaisen kehityksen ja riskien hallinnan. Pitkän kantaman tiedonsiirtoratkaisuun pohjautuvalla toteutukselle on laaja tuki osittain epämääräisestä tai puutteellisesta sääntelykehikosta huolimatta, koska sen nähdään olevan kustannustehokas vaihtoehto toteuttaa kansallinen C-ITS-järjestelmä. Yhteistyötä muiden maiden toimijoiden - erityisesti Pohjoismaiden, joiden kanssa tällaisesta on jo aiempaa kokemusta - pidetään hyvin potentiaalisena lähestymistapana, sillä se mahdollistaa kustannusten ja asiantuntemuksen jakamisen eri toimijoiden kesken. Tällainen yhteistyö luo laajemmat resurssit ja vahvemman perustan palveluiden kehittämiselle. Lisäksi yhteiskehittämismallilla voidaan tukea kotimaisten toimijoiden mahdollisuuksia päästä markkinoille ja edistää heidän kilpailukykyään kansainvälisesti. Kansallisen yhteyspisteen (NAP – National Access Point) hyödyntäminen C-ITS-palveluiden lähtötietojen kokoamisessa ja tuottamisessa nähtiin myös hyvänä toimintamallina, sillä se edesauttaa lähtötietojen laadunvarmistuksessa sekä on yksikköoperaattorivastuiden näkökulmasta suoraviivaisin malli.

11 Ehdotus C-ITS-järjestelmän toteutusmalliksi Suomen oloissa

11.1 Toteutusehdotuksen päälinjat

Ehdotus C-ITS-palveluiden käyttöönoton valmiuksien edistämiseksi perustuu selvitystyöryhmän näkemyksiin sekä sidosryhmille järjestetyn asiantuntijatyöpajan tuloksiin. Selvitystyöryhmän näkemykset pohjautuvat työn aikana tehtyyn kirjallisuuskatsaukseen, ulkoisiin asiantuntijahaastatteluihin sekä asiantuntijoiden omaan kokemukseen aihepiirin teemoista. Asiantuntijatyöpajan avulla puolestaan kartoitettiin keskeisimpien toimijoiden näkemyksiä ja odotuksia sekä C-ITS-palveluiden toteutuksen kansallista tahtotilaa. Alla on listattu kansallisen C-ITS-toteutusehdotuksen päälinjat ja niitä on käsitelty jäljempänä tarkemmin.

- Toteutus perustuu pitkän kantaman tiedonsiirtoratkaisuun.
- Toteutusta edistetään vaiheittain, mutta toimet aloitetaan välittömästi.
- Avoimen lähdekoodin yhteisöön pohjautuvaa kehittämisen mallia hyödynnetään mahdollisuuksien mukaan.
- Toteutuksessa huomioidaan käyttöönottoon liittyvät kaupalliset strategiat.
- Kansallinen yhteyspiste (NAP – National Access Point) on keskeinen osa kansallista C-ITS-palveluiden käyttöönottoa.
- Kansallinen C-ITS-toteutus vaatii julkisen sektorin toimia.
- Laadukkaat lähtötiedot ovat ensiarvoisen tärkeitä.
- Yksityisyyden suojan varmistamiseksi toteutus aloitetaan I2V-viesteistä (Infra-to-Vehicle), jotka eivät sisällä henkilötietoa.

Kuva 18 havainnollistaa tämän luvun ehdotuksen mukaisen kansallisen C-ITS-toteutuksen arkkitehtuurin ja toimintaperiaatteen. Kohdat 2A, 2B ja 2C esittävät vaihtoehtoisia toimintamalleja. Myös kohdat 5A ja 5B ovat vaihtoehtoisia, mutta eivät toisiaan poissulkevia toimintamalleja.

1. Tieto maantie- tai katuverkon tapahtumasta tuotetaan digitaalisessa muodossa. Kyseessä voi olla mikä tahansa palvelu, tässä esimerkissä urakoitsijan tuottama tieto tietyömaasta. Tiedot voivat olla urakoitsijan itse määrittämässä formaatissa tai tunnetussa liikennetietojen välittämiseen kehitetyssä formaatissa, kuten DATEX2.

2A. Tieto välitetään urakoitsijan järjestelmistä kunnan C-ITS-keskusyksikköön. Tähän voidaan hyödyntää DATEX2-rajapintaa tai keskusyksikköoperaattorin ratkaisua tietojen muuntamiseen soveltuvaan formaattiin urakoitsijan käyttämästä.

2B. Tieto välitetään urakoitsijan järjestelmistä kansalliseen C-ITS-keskusyksikköön. Tähän voidaan hyödyntää DATEX2-rajapintaa tai keskusyksikköoperaattorin ratkaisua tietojen muuntamiseen soveltuvaan formaattiin urakoitsijan käyttämästä.

2C. Tieto välitetään urakoitsijan järjestelmistä kansalliseen yhteyspisteeseen. Tähän voidaan hyödyntää DATEX2-rajapintaa tai kansallisen yhteyspisteen

operaattorin ratkaisua tietojen muuntamiseen soveltuvaan formaattiin urakoitsijan käyttämästä.

3. Kansallinen yhteyspiste toimittaa tiedot C-ITS-keskusyksikölle. Tietosisältö voidaan muuntaa C-ITS-keskusyksikön tukemaan muotoon, mutta varsinaisen viestien allekirjoituksen voi tehdä vain C-ITS-keskusyksikkö.

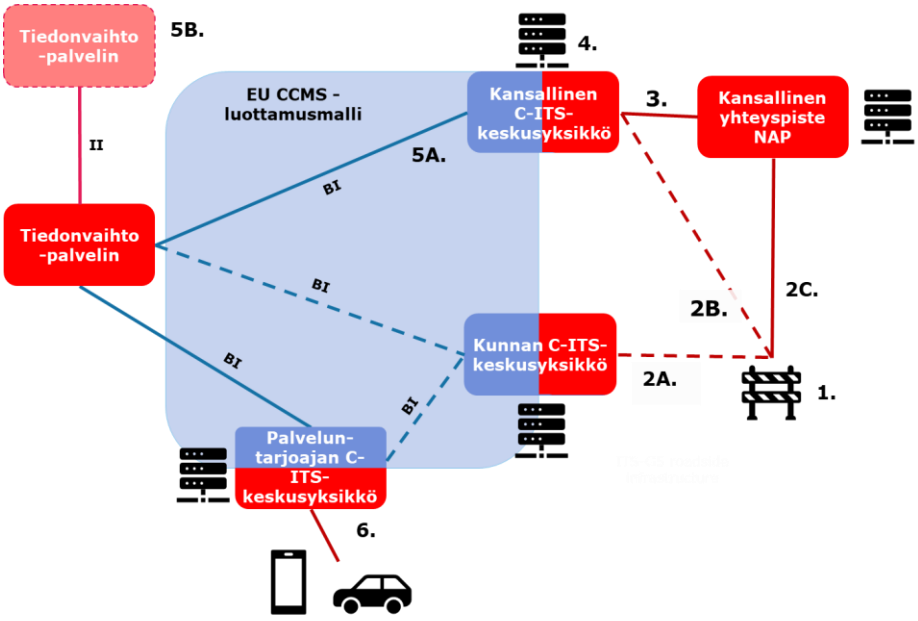
4. Keskusyksikkö muodostaa C-ITS-viestin. Vastaanottamansa tietosisällön perusteella muodostetaan ETSI-standardin mukainen C-ITS-viesti, johon lisätään myös IP-pohjaisessa tiedonsiirrossa tarvittavat otsikkokentät.

5A. C-ITS-viesti välitetään keskusyksiköiden välillä BI-protokollan mukaisesti. Tällöin jokaisen yhteen liitettävän C-ITS-keskusyksikön välille täytyy rakentaa BI-protokollan mukainen rajapinta.

5B. C-ITS-viesti välitetään tiedonvaihtopalvelinten välillä II-protokollan mukaisesti. Tällöin jokaisen yhteen liitettävän C-ITS-keskusyksikön välille ei tarvitse rakentaa omaa rajapintaa, vaan tiedonvaihtopalvelin huolehtii yhdistettävyydestä toisiin keskusyksiköihin.

6. C-ITS-viesti välitetään loppukäyttäjälle. Palveluntarjoaja operoi omaa C-ITS-keskusyksikköään ja välittää C-ITS-viestit loppukäyttäjille.

Havainnekuvan mukainen C-ITS-toteutuksen arkkitehtuuri esittää myös EU:n C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) rajat, eli milloin C-ITS-viestien on oltava allekirjoitettuja (sinisellä taustalla oleva alue kuvassa 18). Käytännössä tämä jättää paljon vapauksia esimerkiksi tienpitäjälle tietojen tuottamisessa sekä palveluntarjoajille viestien välittämisessä loppukäyttäjille. Vaikka tiettyjä osia kuvan arkkitehtuurista eivät C-ITS-turvatunnusten hallintajärjestelmän määritelmät koske, niin se ei silti poista C-ITS-yksikköoperaattorin vastuita C-ITS-viestien muodostamiseksi käytetyn tiedon luottamuksellisuudesta, eheydestä tai käytettävyydestä. Myös tiedonvaihtopalvelimet ovat kyseisen luottamusmallin ulkopuolella, sillä ne eivät muodosta tai allekirjoita C-ITS-viestejä, vaan ainoastaan välittävät niitä.



Kuva 18. Havainnekuva kansallisesta C-ITS-toteutuksen arkkitehtuurista.

Toteutus perustuu pitkän kantaman tiedonsiirtoratkaisuun

Selvitystyön tutkimuskysymykset ovat ohjanneet työtä tarkastelemaan nimenomaan pitkän kantaman tiedonsiirtoratkaisuun perustuvaa C-ITS-toteutusta. Pitkän kantaman tiedonsiirtoon tukeutumista puoltaa kansallisen tahtotilan yhteydessä hallinnonalan keskeisissä julkaisuissa ja strategisissa dokumenteissa tunnistettu kytkös matkaviestinverkkoteknologioiden soveltuvuudesta liikennevertikaaleille liikenteen digitalisaation edistämiseksi. Tämän voidaan katsoa tukevan C-ITS-järjestelmien kehittämisen näkökulmasta nimenomaan pitkän kantaman tiedonsiirtoon pohjautuvaa toteutusmallia. Matkaviestinverkkoyhteydet ovat oleellisessa osassa pitkän kantaman tiedonsiirtoon perustuvaa toteutusta, ja verkon kyvykkyyttä sekä kehityssuuntia on tarkemmin tarkasteltu tämän selvitystyön luvussa 9. Tietyistä ongelmakohdistaan huolimatta jo nykyisellään matkaviestinverkot tarjoavat varsin kattavan ratkaisun C-ITS-palveluiden tarpeisiin. Lisäksi voidaan olettaa, että tulevaisuuden verkkoteknologioiden kehitys ja uudet ominaisuudet tulevat tukemaan C-ITS-palveluiden toteuttamista pitkän kantaman tiedonsiirtoon perustuvassa ratkaisussa. Tässä selvitystyössä ei kuitenkaan ole varsinaisesti arvioitu eri tiedonsiirtoteknologioiden kyvykkyyttä toteuttaa yksittäisiä C-ITS-palveluita (luvussa 1.2 esitettyjen rajausten mukaisesti) tai eri teknologioiden mahdollisia kustannusvaikutuksia toteutukseen.

Pitkän kantaman tiedonsiirtoon tukeutuminen tarkoittaa käytännössä sitä, että toteutus perustuu IP-verkossa sijaitsevien C-ITS-keskusyksiköiden väliseen tiedonsiirtoon sekä matkaviestinverkkojen hyödyntämiseen tien- ja kadunvarren laitteiden sekä loppuasiakkaiden saavuttamisessa. Lisäksi tarvitaan tiedonvaihtopalvelin, joka mahdollistaa liittymisen osaksi Euroopan laajuista C-ITS-ekosysteemiä. Toiminnan alkuvaiheessa tämä voi olla myös Suomen ulkopuolinen tiedonvaihtopalvelin, johon liittyminen parantaisi yksittäisen Suomessa operoivan C-ITS-keskusyksikön viestien löydettävyyttä. Tarvittavia käytännön kokonaisuuksia ovat siis keskusyksikön hankinta tai kehittäminen sekä käyttöönotto ja operointi, yksikköoperaattorin tietoturvallisuuden hallintajärjestelmän käyttöönotto, varmennepalveluiden käyttöönotto sekä tiedonvaihtopalvelimen hankinta tai kehittäminen sekä käyttöönotto ja operointi. Näiden toteuttamiseen liittyviä konkreettisempia toimia on esitelty tarkemmin seuraavassa toimeenpanoa ja organisoitumista käsittelevässä luvussa 11.2.

Toteutusta edistetään vaiheittain, mutta toimet aloitetaan välittömästi

Edellä mainitun mukainen pitkän kantaman tiedonsiirtoon perustuva kansallinen C-ITS-toteutus edellyttää useita hankintoja tai kehityshankkeita. Hankinnan valmistelusta käyttöönottoon ja ylläpitoon tulee varata aikaa, ja tästä syystä suosituksena on aloittaa valmisteluun liittyvät toimet välittömästi. Toisaalta erityisesti pitkän kantaman tiedonsiirtoon perustuvaan toteutukseen liittyen on tässä selvityksessä esitetty määrittelyyn liittyviä kohtia, joiden odotetaan vielä tarkentuvan C-Roads-työryhmien työn edetessä. Tästä syystä kansallista C-ITS-järjestelmää on kokonaisuudessaan haasteellista suunnitella täysin valmiiksi, ja täten suositus on edistää kehitystä vaiheittain samalla aktiivisesti keskeisille määrittely- ja yhteistyöfoorumeille osallistuen. Tarkempi kuvaus toimeenpanosta ja organisoitumisesta on esitetty seuraavassa luvussa 11.2.

Kansallisessa toteutusmallissa on syytä arvioida mahdollisuuksia C-ITS-keskusyksikön ja tiedonvaihtopalvelimen hankintaan kaupallisena ratkaisuna, oman kehityksen avulla toteutettuun räätälöityy ratkaisuun tai avoimen lähdekoodin

yhteisöön pohjautuvaan kehitysmalliin. Kaikilla näillä vaihtoehdoilla on omia vahvuuksia ja haasteita.

Kaupallisilla tuotteilla on yleisesti jatkuva markkinoiden ja regulaation vaatimusten mukainen kehitys- ja tuotetuki, sillä kaupallisilla toimijoilla on intressi pitää tuotteensa vaatimusten mukaisina. Toimijoiden välinen kilpailu kannustaa toimijoita kehittämään tuotteitansa ja hillitsemään kustannuksia. Kaupallisen ratkaisun hankinta sisältää myös tyypillisesti raskaat järjestelmän alusta- ja käyttöpalveluosuudet, kuten palvelinsali-, pilvipalvelu-, tietoliikenne-, tietoturva-, valvonta-, ylläpito- ja käyttötukipalvelut, jolloin tilaajan ei tarvitse hankkia näitä osuuksia erillisten sopimusten kautta. Vaikka kaupallinen tuote sisältää yleensä yleisten vaatimusten mukaiset ratkaisun ominaisuudet, sen käyttöönotto tyypillisesti vaatii myös valmiin ratkaisun käyttöönottoon liittyvää lokalisointia ja integrointia. Yhtenä esimerkkinä on yleensä toimintaympäristöön liittyvien tietolähteiden integrointi. Mikäli tilaajalla on lokalisointiin ja integrointiin liittyvät vaatimukset selvillä kilpailutuksen yhteydessä, ne voidaan sisällyttää tarjouspyyntöön tuotteeseen ja sen käyttöönottoon liittyviksi vaatimuksiksi.

Kaupalliset ratkaisut sisältävät kaikkien vaihtoehtojen tavoin myös riskejä. Yksi keskeinen riski on, ettei markkinoille synny monipuolista, kehittyvää ja useita vaihtoehtoja sisältävää ratkaisutoimittajien verkostoa. Tämä tyypillisesti takaa, että markkinoilla on riittävästi kilpailua, nopeasti kehittyviä ratkaisuja sekä ratkaisuiden erottautumiseen tähtäävää yritysten aktiivista innovointia, jotka pitävät hintatason kohtuullisena. Mikäli näin ei tapahdu, niin potentiaalisia riskejä ovat yleiseen kustannustasoon ja tuotteiden hidastuneeseen kehitykseen liittyvät riskit. Tämä saattaa johtaa riippuvuuteen toimittajasta, mikä voi johtaa kustannusten nousuun, jos ratkaisua ei ole helppoa kilpailuttaa tai sen kilpailuttaminen on hankalaa esimerkiksi yhteentoimivuusongelmien tai korkeiden vaihtokustannusten takia.

Toki on hyvä tiedostaa, että mikäli tuotehankinnalle nähdään vaihtoehtona oma räätälöidyn ratkaisun toteutus, niin tämäkään malli ei ole riskitön. Keskeisenä riskinä on elinkaarikustannusten hallinta, sillä ratkaisu tulee vaatimaan sen ensimmäisen version valmistumisen ja käyttöönoton jälkeen jatkuvaa kehitystä, joka tulee ostaa erillisenä asiantuntijatyönä. Laajojen toteutusten osalta asiantuntijoilla voi mennä merkittäviä aikoja ottaa ratkaisu haltuun mahdollisessa ohjelmistokehityskumppanin tai pelkästään keskeisten kehittäjien vaihdostilanteissa. Ohjelmistokehityskumppanin vaihtaminen voikin olla joskus huomattavan monimutkainen ja kallis prosessi. Jatkuvan oman räätälöidyn ratkaisun kehityksen lisäksi oman ratkaisun alusta-, käyttö- ja ylläpitopalvelut tulee hankkia erikseen ja ne on hyvä huomioida vertailtaessa eri ratkaisujen kustannustasoja.

Tuotepohjaisten ratkaisujen vaihtamista helpottaa erityisesti C-ITS-järjestelmien taustajärjestelmiin (C-ITS-keskusyksiköt ja tiedonvaihtopalvelimet) liittyvät Euroopan laajuiset määrittelyt ja standardit, jotka varmistavat eri toimittajien ratkaisujen välisen yhteentoimivuuden. Tuotepohjaisten ratkaisujen vaihtoon liittyen on huomioitava ja vaadittava uudelta ratkaisutoimittajalta integraatioiden tekeminen kansallisiin lähtötietorajapintoihin (tuoteratkaisun sovittaminen kansalliseen toimintaympäristöön eli lokalisointi). Tämä antaa hyvät edellytykset kaupallisille toimijoille kehittää tuotteita ja ratkaisuja, jotka ovat käyttöönotettavissa laaja-alaisesti Euroopassa.

Myöskään huoltovarmuusnäkökulmasta asia ei ole yksiselitteinen, sillä suurilla kansainvälisillä toimijoilla voi olla paremmat valmiudet huolehtia järjestelmien toimintakyvystä ja palautumisesta häiriötilanteissa. C-ITS-viestien merkitys osana kriittistä infrastruktuuria voidaan kuitenkin etenkin toteutuksen alkuvaiheessa nähdä lievänä, mikäli palveluilla on ennemmin informatiivinen kuin turvallisuuskriittinen tai ohjaava rooli (kuten luvussa 9.1 on palveluiden luonnetta pohdittu).

C-ITS-ekosysteemin toteutuksessa on syytä kiinnittää erityistä huomiota skaalautuvuuteen eli mahdollistaa useampien keskusyksiköiden mukaan liittyminen myöhemmissä vaiheissa. Vaiheittainen toimeenpano voidaan aloittaa kansallisen C-ITS-keskusyksikön toteutuksella, joka vastaa esimerkiksi maantieverkon C-ITS-palveluista. C-ITS-toteutuksen edetessä on tässä selvityksessä tunnistettu kuitenkin tilanteita, jolloin esimerkiksi kunnilla voi tulla kyseeseen oman C-ITS-keskusyksikön käyttöönotto. Kaupunkikohtainen C-ITS-keskusyksikkö tulee kyseeseen silloin, kun kaupunki haluaa tarjota kaupungin alueella liikkuville monipuolisempia C-ITS-palveluita kuin kansallinen yksikkö (esimerkiksi katuverkon liikenteen ruuhkautumisesta tai lähestyvästä hälytysajoneuvosta varoittavia palveluita). Tällaista tilannetta on kuvattu esimerkinomaisesti tarkemmin luvussa 6.5.

Avoimen lähdekoodin yhteisöön pohjautuvaa kehittämisen mallia hyödynnetään mahdollisuuksien mukaan

Selvitystyössä tunnistettiin asiantuntijahaastatteluiden perusteella, että kaupalliset ratkaisut eivät ole kaikilta osin vielä täysin kypsiä, erityisesti pitkän kantaman tiedonsiirtoon perustuvien ratkaisujen määrittelyyn liittyvien puutteiden takia. Tästä syystä hankintaan sisältyy aina jossain määrin omaa resursointia sekä tietyllä tavalla riskin ottoa. Toisaalta selvitystyössä on myös tunnistettu, että Euroopan laajuisen C-ITS-järjestelmiin liittyvän standardoinnin seurauksena kaikilla mailla on hyvin samanlaiset vaatimukset C-ITS-yksiköille sekä tiedonvaihtopalvelimelle. Tämä piirre mahdollistaa myös eri maiden välisen yhteisökehittämisen, jota voidaan toteuttaa Euroopan unionin avoimen lähdekoodin hyödyntämisen strategian mukaisesti avoimen lähdekoodin yhteisötoimintana.

Avoimen lähdekoodin yhteisötoiminnan tarkempi tutkiminen ei sinänsä ole osa tätä selvitystyötä, mutta sen hyödyntämistä on kuvattu selvitystyön luvussa 7 osana tiedonvaihtopalvelimen toteutusvaihtoehtojen tarkastelua. Sama kehitysmalli soveltuu yhtä hyvin myös C-ITS-keskusyksikön kehittämiseen. Tässä selvityksessä tunnistettiin useita avoimen lähdekoodin yhteisöön pohjautuvan kehittämisen hyötyjä, jotka tekevät siitä houkuttelevan vaihtoehdon. Tämän vaihtoehdon avulla voidaan mm. jakaa kehittämiskustannuksia sekä osaamista. Avoimen yhteisön kehittäminen voi myös taata hyvin toimivan kehitystyön hallinnon sekä laaduntarkkailuprosessit. Lisäksi samaan toteutukseen sitoutuneiden useamman toimijan ratkaisulla on todennäköisesti suurempi painoarvo yhteistyöfoorumeilla, joissa C-ITS-sääntelyä kehitetään. Myös asiantuntijatyöpajassa tunnistettiin nämä avoimen lähdekoodin yhteisön kehittämiseen liittyvät hyödyt laajasti. Haasteina tämän kehitysmallin osalta tunnistettiin mm. mahdollisesti raskas yhteisön perustamiseen liittyvä hallinnollinen työ, kuten kaikkia maita tyydyttävä yhteisön toiminnan hallintomalli, kustannuksista sopiminen sekä kehitystyöhön liittyvä yhteinen tavoitetila ja prioriteetit.

Toteutuksessa huomioidaan käyttöönottoon liittyvät kaupalliset strategiat

Julkishallinnon roolia tällaisten kehityshankkeiden toteutuksessa on syytä tarkastella. Olennainen kansallisen markkinan ominaisuus on asiakkaiden rajallinen määrä. Mikäli julkishallinto kehittää C-ITS-keskusyksikköratkaisun omana kehityshankkeena (eli kilpailuttaa kehittäjätiimin, joka toteuttaa räätälöidyn ratkaisun) eikä hanki sitä kaupallisen toimijan tuotepohjaisena ratkaisuna, niin on riskinä, ettei Suomeen välttämättä synny kaupallisia ratkaisuja tarjoavia toimijoita.

Kotimarkkina toimii tärkeänä referenssinä vientimarkkinoille tähtääville kotimaisille yrityksille. Liikennealan yritysten digitaalisista palveluista ja alustoista odotetaan kasvavissa määrin vientitoimintaa, joka tukee Suomen talouskasvua ja vahvistaa Suomen edelläkävijyyttä digitalisaation hyödyntäjänä sekä kestävän kehityksen edistäjänä. Tätä toimintaa edistämään on myös vuonna 2024 perustettu Fintrafficin koordinoima liikennedatan vientiklusteri, jonka tavoitteena on Suomessa kehitettyjen liikennedatan palveluiden laaja-alainen käyttöönotto Euroopassa, ja tätä kautta aukeavat liiketoimintamahdollisuudet suomalaisille alan yrityksille. Klusteri pyrkii mahdollistamaan suurempia vientihankkeita, jotka ovat yksittäisten yritysten tarjoaman tai kyvykkyyksien ulottumattomissa (Vientiklusteri, n.d.). Yksi klusterin yritysten alkuvaiheen yhteistarjoaman kokonaisuuksista on nimenomaan liikkumispalvelut ja -tieto, joten C-ITS-kehityksen ottaminen osaksi vahvemmin vientiklusterin toimintaa voisi olla ratkaisu tukea sekä kansallista C-ITS-kehitystä että alan yritysten toimintaa. Kansallisessa toteutusmallissa suositellaan, että erilaisten etenemishaarojen pohdinnassa pyritään huomioimaan kotimaisten teknologiatoimijoiden tuote- ja palvelupohjainen C-ITS-ratkaisujen kehittyminen.

Selvitystyössä on myös tuotu esille kansallinen kaupallinen strateginen ajattelu myös avoimen lähdekoodin yhteisötoimintaan liittyen. Tässä ajattelussa korostuu avoimen lähdekoodin yhteisön toiminnan suunnittelu yhteistyössä paikallisen yksityisen sektorin kanssa. Mallissa keskeistä on jo kehitystyön aloituksen yhteydessä pyrkiä luomaan strategia siitä, minkälaiset lopullisen ratkaisun osuudet toteutetaan avoimen lähdekoodin yhteisössä (esimerkiksi keskeiset ydinteknologiat ja alustat), ja mitkä osuudet jätetään yksityisen sektorin toteutettavaksi (lopullinen tuotteistaminen). Nämä yksityisen sektorin ominaisuudet voivat sisältää esimerkiksi lopullisen ratkaisun liiketoimintakriittiset ominaisuudet, omat innovaatiot sekä tyypillisen avoimen lähdekoodin ratkaisuihin liittyvän kaupallisen ajattelun, eli tuottaa avoimeen lähdekoodiin pohjautuvalle lopulliselle ratkaisulle tuotetuki. Tämän ajattelun avulla julkishallinto voi vahvasti hallita ratkaisun kehitystä ja vaatia tuotepohjaisessa hankinnassa, että hankittavan tuotteen tulee pohjautua kyseiseen avoimen lähdekoodin hyödyntämiseen osana lopullista ratkaisua (kilpailutukseen liittyvä teknologiavaatimus). Tässä mallissa alan yritysten olisi mahdollista osallistua avoimen lähdekoodin yhteisöön, jolloin ne olisivat mukana avoimen yhteisön mukaisessa kehitystyössä ja pyrkisivät tuotteistamaan markkinoille avoimen koodin pohjalta omia ratkaisuja. Mallissa julkinen ja yksityinen sektori ovat parhaimmillaan aktiivisesti mukana ratkaisun kehityksessä, avoin lähdekoodi mahdollistaisi yksityiselle sektorille tuotteiden ja palveluiden syntymisen, joille syntyisi myös samalla kansallisia referenssejä, kun julkishallinto ei ottaisikaan käyttöön varsinaista avoimen lähdekoodin ratkaisua (sen ei alkuperäisen ajatuksen mukaisesti edes ole tarkoitus synnyttää lopullista ratkaisua), vaan sen pohjalta tuotteistettuja yksityissektorin ratkaisuja.

Kansallinen yhteyspiste (NAP – National Access Point) on keskeinen osa kansallista C-ITS-palveluiden käyttöönottoa

Tämän selvitystyön yhtenä lopputuloksena esitetään, että kansallinen yhteyspiste (NAP) tulee käsittää keskeisenä osana kansallista C-ITS-ekosysteemiä ja -kehitystä. Itsenäisenä järjestelmänä se ei varsinaisesti ole osa C-Roadsin määritysten mukaista C-ITS-järjestelmää, eikä siihen siten kohdistu samoja vaatimuksia. Kansallisella yhteyspisteellä on kuitenkin laajempi rooli tieliikenteeseen liittyvien tietojen jakelun suhteen sekä merkittävä rooli ITS-toimialan ja siihen liittyvien järjestelmien kehityksessä, joten sen kehittämiseen kannattaa investoida.

Kansalliseen yhteyspisteeseen (NAP) toimitettavat tietotyypit ovat monissa tapauksissa sellaisia (esimerkiksi tosiaikaiset liikennetiedot sekä liikenteen turvallisuustiedot), joiden avulla voidaan muodostaa C-ITS-viestejä. C-ITS-keskusyksiköt voivat lukea kansallisen yhteyspisteen kautta näitä tosiaikaisia liikennejärjestelmän tilannetietoja, joita ovat esimerkiksi liikennemerkkitiedot vaikutusalueineen, sääolosuhteet, häiriötilanteet tai tietyömaiden sijainti. Näiden tietojen avulla voidaan muodostaa kuhunkin aiheeseen liittyviä C-ITS-viestejä, joita C-ITS-palveluntarjoajat voivat tarjota loppukäyttäjilleen. Informaatio- ja varoitusviestejä voidaan esittää loppukäyttäjille palveluntarjoajien kehittämien C-ITS-mobiilisovellusten avulla tai välittämällä tiedot suoraan ajoneuvoille, joissa on jo integroitu C-ITS-ajoneuvoyksikkö.

Kansallisen yhteyspisteen voidaan katsoa palvelevan tästä näkökulmasta koko liikenteen toimialaa, ei pelkästään C-ITS-ekosysteemiä, joten sen rooli on laaja. Kansallinen yhteyspiste (NAP) on digitaalisen infrastruktuurin kansallinen alustapalvelu, joten yksittäisten toimijoiden ei tarvitse investoida oman ratkaisun toteuttamiseen liikennetietojen hyödyntämiseksi. Jokaisella kaupungilla on oikeus ja mahdollisuus hyödyntää kansallista yhteyspistettä kehittääkseen oman liikennejärjestelmänsä palvelutasoa. Vapaasti käytettävä infrastruktuuri, jonne erilaiset liikennetiedot ovat laajasti toimitettavissa, on näin ollen kansallisessa yhteyspisteessä olemassa, ja C-ITS on yksi konkreettinen tapa hyödyntää tätä infrastruktuuria. C-ITS mahdollistaa myös toimintojen, jotka on tähän asti toteutettu kansallisilla ratkaisuilla, kuten hälytysajoneuvojen etuusjärjestelyt, toteuttamisen C-ITS-keskusyksikön kautta. Tämän mahdollistaa sen, että älykkäitä liikennepalveluita voidaan teknisesti toteuttaa ja hallita yhdestä pisteestä.

Kansallinen C-ITS-toteutus vaatii julkisen sektorin toimia

Selvitystyön tulokset on kohdennettu pääasiassa julkisen sektorin toimijoille huomioiden kuitenkin myös kaupallisten palveluntarjoajien ja muun yksityisen sektorin näkökulmat. Toimivan C-ITS-järjestelmän toteutus kokonaisuudessaan edellyttää, että kaupallisia toimijoita saadaan mukaan. Julkisen sektorin toimijoilla on kuitenkin merkittävä rooli C-ITS-ekosysteemissä, sillä julkisen sektorin toimijat omistavat ja hallinnoivat suurta osaa liikenneinfrastruktuurista, kuten tie- ja katuverkostoja sekä liikennevaloja, jotka ovat olennaisia C-ITS-palvelutoteutusten toiminnan kannalta. Rooli korostuu erityisesti taustalla tarvittavan digitaalisen infrastruktuurin rakentamisessa, jolla tässä yhteydessä tarkoitetaan esimerkiksi C-ITS-keskusyksiköitä sekä tiedonvaihtopalvelinta. Hallinnolliset roolit, kuten varmenteiden hallinta ja C-ITS-yksiköiden luvitus, on myös selkeää pitää julkisen sektorin toimijoilla.

Loppukäyttäjäpalveluiden tarjoaminen ei ole yksiselitteisesti kuvattavissa julkisen sektorin tai yksityisen sektorin toimena, vaan molemmilla tahoilla on tässä roolissa omat vahvuutensa. Yksityisen sektorin palveluille on ominaista, että ne tarjotaan tehokkaasti kilpailuympäristössä, jossa markkinamekanismit säätelevät tarjontaa ja hinnoittelua. Tällöin kilpailuasetelma voi parantaa esimerkiksi palveluiden laatua ja kustannustehokkuutta. Nykyisessä markkinatilanteessa monet tienkäyttäjien loppukäyttäjäpalveluita tarjoavista tahoista ovat yksityisiä yrityksiä. Toisaalta tiettyjen palveluiden osalta myös julkisella sektorilla voi olla hyvät edellytykset tarjota loppukäyttäjäpalveluita. Esimerkiksi Fintraffic Mobiili -sovellus tavoittaa jo nyt lukuisia suomalaisia tienkäyttäjiä ja auttaa liikennetilannetiedon jakamisessa. C-ITS-kehityksen näkökulmasta kaupalliset toimijat tarvitsevat joka tapauksessa varmuutta ja pidemmän tähtäimen näkymää investoinneilleen. Julkinen sektori voi tarjota näitä näkymiä investoimalla C-ITS-järjestelmän taustainfrastruktuurin kehitykseen. Ilman julkisen sektorin panostuksia C-ITS-toteutuksen aikajänne on pidempi ja jopa epävarma.

Laadukkaat lähtötiedot ovat ensiarvoisen tärkeitä

Laadukkaiden lähtötietojen merkitys korostuu pitkän kantaman tiedonsiirtoon perustuvassa C-ITS-toteutuksessa. Tämä johtuu siitä, että C-ITS-keskusyksiköiden operaattorit ovat vastuussa C-ITS-viestien muodostamisen yhteydessä käytettävien lähtötietojen luotettavuudesta C-ITS-turvallisuuspolitiikkadokumentin mukaisesti (katso C-ITS-yksiköiden operointia käsittelevä luku 4.2). Tietojen ajantasaisuuden ja laadun varmistus ovat siis keskeisiä ratkaistavia asioita, jotta esimerkiksi kansalliseen yhteyspisteeseen (NAP) kerättyjä tietoja ja sitä kautta muodostettuja C-ITS-viestejä voitaisiin pitää varteenotettavana toteutusmallina C-ITS-palveluille.

Laatumäärittelyä kehitetään eri foorumeilla. Esimerkiksi NAPCORE-hankkeen kanssa läheistä yhteistyötä tekevä, EU:n tienpitäjistä ja operaattoreista koostuva RTTI-työryhmä (RTTI Task Force), on aloittanut RTTI-tietojen tähtiluokitukseen (EURO NCAP -törmäystestien mukaisesti asteikolla 1–5 tähteä arvioiden) perustuvan laatumäärittelyn. Työryhmän työskentely perustuu TISA (Traveller Information Services Association) -yhdistyksessä toimivien tieliikenteen informaatiopalveluiden palveluntarjoajien ehdotukseen. Tämän selvitystyön toteuttamisen aikaan asia oli RTTI-työryhmän työstettävänä, mutta virallinen laatukriteeristö se ei vielä ole. Ajoneuvoteollisuuden, liikenteen informaatiopalveluiden tuottajien sekä tienpitäjien liikenteenturvallisuustietojen jakamiseksi perustettu yhteistyöfoorumi Data for Road Safety -ekosysteemi (DfRS-ekosysteemi) on puolestaan kehittänyt SRTI-tietojen laatumäärittelyä. Tämä määrittely perustuu toimijoiden itse suorittamaan datajulkaisuiden laatutason raportointiin ekosysteemissä. Toimijat tekevät ilmoituksen viestikohtaisesti kahdella eri laatutasolla (A ja B). Näiden laatutasojen välillä on tarkkuudessa merkittävä ero. Tämän selvityksen suosituksena on pyrkiä laatutasolla kohti A-luokkaa, ja on jopa kyseenalaista, onko B-luokan laatutaso riittävä C-ITS-viestien muodostamiseksi C-ITS-keskusyksikössä. C-Roads ei ole julkaissut varsinaista C-ITS-palveluiden laatumäärittelyä kuvaavaa dokumentaatiota, mutta palvelu- ja käyttötapauskuvausdokumentti antaa jonkinlaista osviittaa siitä, mitä tietosisällön tulisi olla.

Fintraffic on suomalaisista toimijoista mukana molemmilla yllä mainituista foorumeista. Päällimmäisenä suosituksena on jatkaa aktiivista työtä näillä foorumeilla sekä myös arvioida, ovatko nämä laatumääreet riittävät C-ITS-

keskusyksikköoperaattoreiden toimintaan (C-ITS-turvallisuuspolitiikan vaatimusten täyttämiseksi), mikäli näiden tietojen perusteella muodostettaisiin C-ITS-viestejä.

Yksityisyyden suojan varmistamiseksi toteutus aloitetaan I2V-viesteistä, jotka eivät sisällä henkilötietoa

C-Roads-määrittelyn mukaisesti I2V-tyyppiset (Infra-to-Vehicle) C-ITS-viestit itsessään eivät tietosisältönsä (payload) puolesta sisällä henkilötietoa. Esimerkkejä näistä ovat tietöihin ja keliolosuhteisiin liittyvät varoitusviestit tienpitäjältä ajoneuvoille. Varsinaisen tietosisällön lisäksi C-ITS-viestit sisältävät C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisen lähettäjän julkisen PKI-varmenteen. Tämä varmenne varmistaa tiedon eheyden, mutta samanaikaisesti se avaa teknisen mahdollisuuden varmenteen avulla tunnistaa lähettäjä. Julkisen varmenteen avulla tehtävää seurantaa (esim. ajoneuvo) on kuitenkin rajoitettu yksityisyyden suojaa parantavilla toimilla, joita ovat esimerkiksi usein vaihtuvat varmenteet sekä tietojen lyhyt säilytysaika. Tekninen mahdollisuus lähettäjän tunnistamiseksi syntyy välillisiä ja useita tietolähteitä yhdistelemällä.

Pitkän kantaman IP-pohjaisessa tiedonsiirrossa C-ITS-viestit salataan TLS-protokollan (Transport Layer Security) avulla. Täten TLS-protokolla toimii myös riskienhallintakeinona viestikuoren sisällä kulkevan PKI-varmenteen osalta. IP-osoite itsessään on henkilötietoa ja se on välttämätön viestin välittämiseksi perille. Tätä tietoa kertyy viestinvälittäjille, joiden roolissa esimerkiksi teleoperaattorit toimivat. Teleoperaattoreiden toimintaa säätelee mm. laki sähköisen viestinnän palveluista ja välitystiedon luovutus on sallittua ainoastaan niille tahoille, joilla on oikeus tätä tietoa käsitellä. Teleoperaattorit voivat jakaa ainoastaan anonymisoitua tietoa asiakkaistaan.

Näillä perusteilla yksityisyyden suojan varmistamiseksi C-ITS-toteutuksessa lähtökohtana voisi olla, että erityisesti I2V-tyyppiset C-ITS-viestit pitkän kantaman tiedonsiirrossa eivät ole henkilötietoa eikä niiden välittäminen vaadi oikeudellista käsittelyperustetta. Käsittelyä kuvaava tietosuojalausunto (DfRS-ekosysteemin esimerkin mukaisesti) on kuitenkin syytä laatia kuvaamaan tietojenkäsittelymenettelyä.

Mikäli henkilörekisteri kuitenkin pidetään välttämättömänä muodostaa (jokainen tietoa keräävä ja lähettävä joutuu arvioimaan tämän itse tapauskohtaisesti), niin C-ITS-direktiivin puuttuessa voitaneen käsittelyperusteena I2V-tyyppisissä C-ITS-viesteissä käyttää *yleistä etua*. Yleinen etu vaatii perusteeksi lainsäädännön, joka määrittää kyseisen käsittelyn tarpeellisuuden ja kategorian. Lainsäädännöllisen perusteen tulee olla tarpeeksi tarkka ja yksityiskohtainen, jotta voidaan varmistaa, että käsittely on oikeutettua. Tähän voisivat soveltua Tieliikennelaki (729/2018), Laki Väylävirastosta (862/2009) tai Laki liikenteen palveluista (320/2017). Euroopan laajuisen C-ITS-toteutuksen kannalta oletuksena on, että EU-tason sääntely tuottaa sovellettavan käsittelyperusteen, esimerkiksi C-ITS-järjestelmien toteutusta koskevan delegoidun asetuksen yhteydessä.

11.2 Toimeenpano ja organisoituminen

Tässä luvussa kuvataan konkreettisemmin, miten edellisessä luvussa 11.1 esitetty ehdotus kansallisesta C-ITS-palveluiden arkkitehtuurin toteutusmallista toimeenpannaan. Toinen keskeinen tämän luvun teema on kuvata, miten hallinnonalan toimijoiden olisi suositeltavaa organisoitua toimeenpanon edistämiseksi. Esitetty organisoitumismalli on toimittajan ehdotus, joka perustuu Kotilainen et al. (2023) esittämään viranomaisten roolijakoon. Esitetty organisoitumismalli ei siten ole hallinnonalan varsinainen suunnitelma organisoitumiseksi.

C-ITS-keskusyksikön toteutus

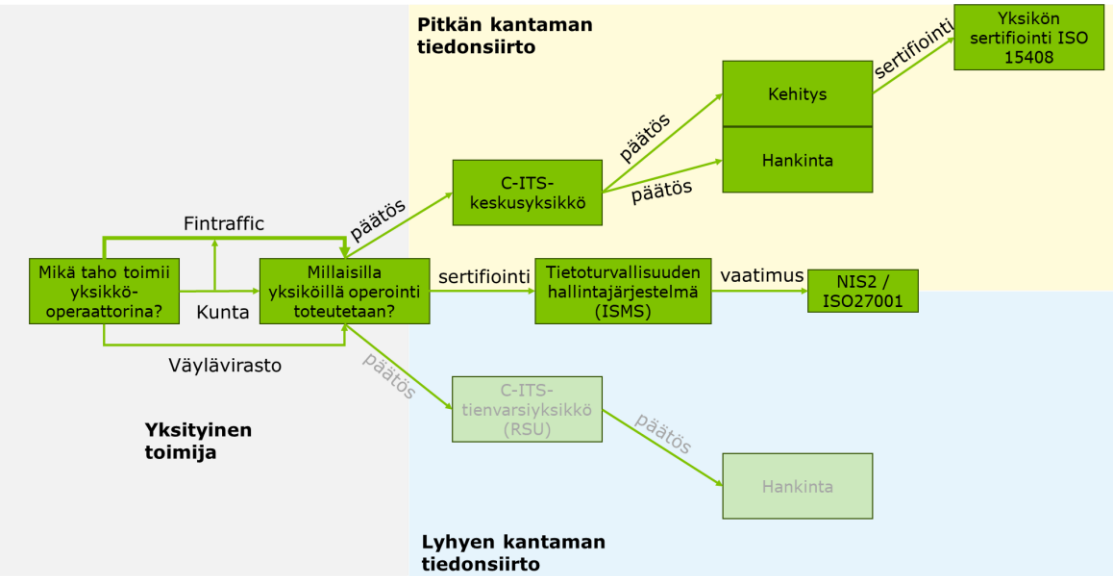
Suositus toteutuspoluksi C-ITS-keskusyksikön käyttöönotolle on esitetty tarkemmin kuvassa 19, jossa tukeudutaan edellisen luvun perusteluihin pohjautuen pitkän kantaman tiedonsiirtoratkaisuun. Tällöin relevantti osuus on kuvan ylempi puolisko. Pitkän kantaman tiedonsiirrolla toteutettu C-ITS-järjestelmä perustuu C-ITS-keskusyksiköiden väliseen tiedonsiirtoon. Keskusyksikkö on ohjelmistopohjainen ratkaisu, ja yksikköoperaattori voi joko kehittää oman yksikön (omana kehitystyönä tai yhteiskehittämismallilla muiden toimijoiden kanssa avoimen lähdekoodin ratkaisuihin tukeutuen) tai hankkia kaupallisen tuotteen.

Kuten tässä selvityksessä on jo aiemmin todettu, niin Euroopan C-ITS-järjestelmän tekninen kehitys, standardointi ja määrittely on hyvin vahvasti perustunut alusta saakka lyhyen kantaman tiedonsiirtoratkaisun hyödyntämiseen. C-Roads-työryhmien pitkän kantaman tiedonsiirtoratkaisun määrittelytyöstä huolimatta kyseisessä mallissa on yhä ratkaisemattomia asioita. Näitä ovat mm. keskusyksiköiden turvaprofiilien puute sekä HSM-moduulien käytön vaatimukset konesaliympäristössä. Osittain tämän puutteellisen määrittelyn takia ei valmiita täysin EU:n C-ITS-turvatunnusten hallintajärjestelmän vaatimuksien (etenkään L2-tason) mukaisia kaupallisia C-ITS-keskusyksiköitä ollut raportin kirjoitushetkellä saatavilla. Tämän selvitystyön yhteydessä on luvussa 5.2 tunnistettu ja esitelty kaupallisia toimijoita, joiden markkinoilla olevat ratkaisut ovat alueellisesti laajaltikin käytössä, mutta eivät täysin vastaa C-Roadsin mukaisia määrittelyitä (esimerkiksi viestien allekirjoittamisen osalta). Kaupallisilla toimijoilla on kuitenkin valmius ja liiketoiminnallinen intressi kehittää tuotteitaan vastaamaan määrittelyitä, joten suositus viranomaistahoille on erityisesti pyrkiä selkeyttämään näitä edellä mainittuja määrittelyitä edistääkseen vaatimusten mukaisten kaupallisten tuotteiden syntymistä.

Edellä mainituiden syiden takia ei suositeltavaksi vaihtoehdoksi voida nostaa yksiselitteisesti yhtä toteutusmallia, vaan suosituksena on selvittää eri vaihtoehtojen toteutettavuutta, kun C-ITS-keskusyksikön toteutus tulee ajankohtaiseksi. C-ITS-keskusyksikön hankkiminen kaupallisena tuotteena edellyttää niihin liittyvien C-Roads-spesifikaatioiden mukaisten vaatimusten tarkentumista, joka mahdollistaisi markkinoilla tarjottavien ratkaisuiden yhdenmukaisuuden. Edellytyksiin toteuttaa C-ITS-keskusyksikkö yhteiskehittämisen kautta vaikuttavat mahdollisuudet löytää muita yhteiskehittämiseen sitoutuvia toimijoita ja muodostaa yhdessä toimiva hallinnollinen ja liiketoiminnallinen kehys.

Kaupallisen valmiin tuotteen hankintaan liittyviä näkökulmia on myös syytä tarkastella kriittisesti. Valmiin tuotteen hankinta ja käyttöönotto sisältävät tyypillisesti myös tuotteen lokalisointiin ja integrointiin liittyviä käyttöönoton yhteydessä toteutettavia räätälöityjä osuuksia. Valmiin tuotteen liian pitkälle viedyssä

räätälöinnissä on kuitenkin syytä olla varuillaan, jotta ratkaisu ei muutu hankalasti vaihdettavaksi ja siten synnytä ns. toimittajaloukkutilannetta. Tuote kannattaakin tämän vuoksi mahdollisuuksien mukaan säilyttää perusominaisuuksiensa osalta määrittelyjen ja standardien mukaisena. Valmiin tuotteen räätälöitävien osuuksien osalta on myös syytä muistaa, että muutoksia voi lähtökohtaisesti toteuttaa vain ohjelmiston omistaja, joten päivitys- ja muokkaustöitä ei täten voi normaalisti kilpailuttaa. Kriittisissä järjestelmissä tuotepohjaisten suljettujen ratkaisujen hankinnassa saatetaan hankintaan sisällyttää erityisehtoja lähdekoodiin aineettomien oikeuksien hallintaan. Näillä niin sanotuilla escrow-lausekkeilla suojataan suljetun ohjelmiston ostajaa tilanteissa, joissa ohjelmistotoimittaja menee konkurssiin tai ei muuten pysty täyttämään ylläpito- ja tukivelvoitteittaan. Lausekkeilla määritellään ne ehdot, joilla ohjelmiston lähdekoodi ja siihen liittyvä dokumentaatio luovutetaan ostajalle.



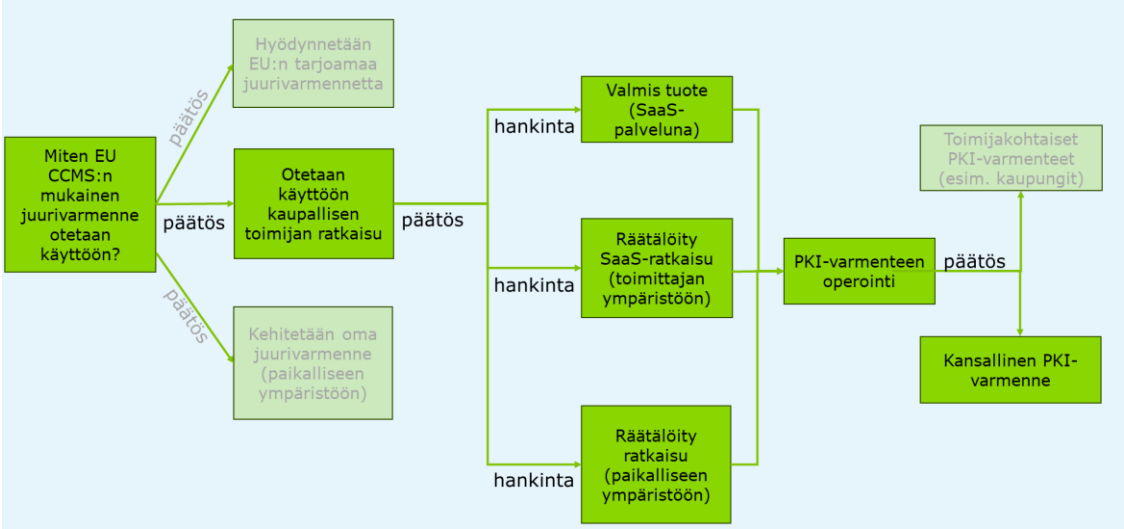
Kuva 19. C-ITS-keskusyksikön toteutus ja operointi (korostettuna suositeltu etenemispolku ja tarkemmin tarkasteltavat vaihtoehdot).

Myös tietoturvallisuuden hallintajärjestelmä on esitetty yllä olevassa kuvassa 19, ja siihen liittyen voidaan todeta, että C-ITS-yksikön tyypistä riippumatta on yksikköoperaattorilla oltava sertifioitu tietoturvallisuuden hallintajärjestelmä. Yleisesti tähän sovelletaan standardin ISO 27001 mukaista hallintajärjestelmää, mutta olennaista liikennepalvelua operoivat tahot voivat soveltaa tietoturvallisuuden hallintaan myös NIS2-kyberturvallisuusdirektiivin mukaisia vaatimuksia. Tietoturvallisuuden hallintajärjestelmä on yksikköoperaattorina toimivan organisaation sisäinen kehityshanke, jonka avulla kehitetään organisaation tietoturvallisuuden johtamista sekä hallintaan liittyviä toiminnallisia prosesseja ja työkaluja. Hallintajärjestelmän tulee ottaa huomioon, ja olla yhdenmukainen, C-ITS-turvallisuuspolitiikan kanssa. Kansallisen C-ITS-keskusyksikön operoijan rooliin liittyen oleellisella taholla, eli Fintrafficilla, oli tämän raportin kirjoittamisen aikaan käynnissä tietoturvallisuuden hallintajärjestelmän kehitystyö.

Varmennepalveluiden käyttöönotto

Tämän selvitystyön luvussa 5.4 esitetyn mukaisesti tulee C-ITS-yksikköoperaattorin tehdä päätös siitä, minkä C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) mukaisen varmennepalveluiden toimittajan kanssa C-ITS-yksiköiden

rekisteröinti ja varmenteiden hallinta toteutetaan. Selvitystyöryhmän suositus varmennepalveluiden käyttöönottamiseksi on esitetty alla olevassa kuvassa 20. Suositus perustuu kaupallisten toimijoiden ratkaisujen hyödyntämiseen. Vaihtoehtoina tälle on hyödyntää EU:n tarjoamaa juurivarmennetta tai kehittää oma ratkaisu. Selvitystyön perusteella voidaan todeta, että Atosin ylläpitämä ilmainen EU-juurivarmennepalvelu on tarkoitettu lähinnä pilotointikäyttöön, eikä sitä ole ollut alun perin tarkoitus käyttää laajamittaisissa lopullisissa L2-tason tuotantoympäristöissä. Tämän EU-juurivarmennepalvelun ylläpito nykyisen sopimuskauden päättymisen (vuoden 2026 loppuun saakka) jälkeen on myös epävarmaa, sillä uuden ITS-direktiivin mukaisissa määrityksissä Euroopan komissiolla ei ole virallista roolia tai vastuuta kyseisen palvelun tuottamisesta. Tästä syystä ei ole suositeltavaa perustaa kansallista varmennepalvelua Atosin ylläpitämän ilmaisen varmennepalvelun varaan, mutta pilotointitarkoituksissa sitä voidaan kuitenkin hyödyntää. Oman juurivarmenteen kehittäminen puolestaan vaatisi merkittävää panostusta, asiantuntijuutta aihepiiristä sekä resursointia niin kehitys- kuin ylläpitovaiheessa, joten sitä ei toteutusmallina voida varauksetta suositella.



Kuva 20. Varmennepalveluiden hankinta ja operointi (korostettuna suositeltu etenemispolku ja tarkemmin tarkasteltavat vaihtoehdot).

Kaupallisilla toimijoilla on tarjota varmennepalveluiden toteuttamiseksi useampia ratkaisuja, jotka vastaavat hyvin C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimuksiin. Pienimuotoisissa tai kertaluontoisissa ympäristöissä on helpointa käyttää juurivarmennepalvelutarjoajien jaettua varmennetta. Tällöin palvelun käyttöönottoon ei tarvita erillisiä varmennepolitiikkaviranomaisen hyväksyttämis- ja auditointitoimia, koska palvelun toimittamiseen käytetty toimintaympäristö on jo läpäissyt nämä vaatimukset. Palveluntarjoajien kanssa käytyjen keskusteluiden perusteella tämä malli on varsin toimiva laajemmissakin toteutusympäristöissä. Suosituksena on ottaa alkuvaiheessa tämä malli kansallisen toteutuksen lähtökohdaksi. Toiminnan laajentuessa tai mahdollisia riskejä tunnistettaessa voidaan toimintaa kehittää asiakastarpeita paremmin vastaaviin ratkaisuihin, jotka on esitelty seuraavissa kappaleissa.

Mikäli tunnistetaan tarve hyödyntää asiakaskohtaista varmennepalvelua, niin voidaan käyttää edelleen SaaS-pohjaista palvelumallia, jossa palvelutoimittaja perustaa asiakkaalle oman erillisen palveluympäristön. Tässä tapauksessa uusi varmennepalvelu rekisteröidään osaksi C-ITS-turvatunnusten hallintajärjestelmää (EU CCMS) ja sen tulee käydä läpi kaikki varmennepalvelutoimittajaa koskevat

hyväksyttämismenettelyt. Palveluntuottaja huolehtii tarvittavista hyväksynnöistä, mutta tämä lisää ympäristöön liittyvää hallinnollista työtä ja kuluja. Tällä mallilla on toteutettu kansallisia (mm. Tšekki), kaupunkikohtaisia (Hampuri) ja organisaatiokohtaisia (mm. Autobahn tai ASFINAG) varmennepalveluita. Jos varmennepalvelun toteuttamisessa SaaS-mallilla nähdään kansalliseen tai organisaation turvallisuuteen liittyviä riskejä, voidaan harkita oman maan tai organisaation sisäiseen konesaliympäristöön perustettavaa juurivarmennepalvelua (paikallinen toteutus). Tämän perustamista varten on kuitenkin varauduttava korkeampiin kustannuksiin, korkean tietoturvallisuustason konesaliympäristön perustamiseen tai hankintaan ja laajempaan omaan rooliin ympäristön hallinnoinnissa sekä C-ITS-turvatunnusten hallintajärjestelmän mukaisissa jatkuvissa hyväksyttämismenettelyissä. Tässä tapauksessa vaatimuksia siis kohdistuu myös palveluympäristön fyysiseen tasoon, ja tämän ympäristön hallinnoinnin vastuu siirtyy enemmän asiakkaalle. Selvityksessä ei ole tunnistettu hallinnointiin tai kyberturvallisuuteen liittyviä tarpeita, joiden perusteella nämä vaihtoehdot olisivat ainakaan C-ITS-toteutuksen alkuvaiheessa perusteltuja.

Varmennepalveluiden operoinnin kannalta voidaan tukeutua joko toimijakohtaisiin PKI-varmenteisiin (esim. kaupunkikohtaiset) tai kansalliseen PKI-varmenteeseen. Kansallisessa C-ITS-toteutuksessa suositellaan tukeutumaan ensisijaisesti kansalliseen PKI-varmenteeseen. Selvitystyössä tunnistetut ehdotetun mallin edut liittyvät yksinkertaisempaan hallintaprosessiin. Kansallinen varmennepalvelutoimittaja tarjoaa paremman hallinnan C-ITS-yksiköiden laajamittaiseen ja pitkäaikaiseen rekisteröintiin verrattuna malliin, jossa kansalliset C-ITS-yksikköoperaattorit valitsevat omatoimisesti toimijakohtaisen PKI-varmenteiden palveluntarjoajan. Varmennepalvelutoimittaja toimii kansallisten viranomaisten kumppanina ja asiantuntijana C-ITS-yksiköiden rekisteröintiin liittyvissä asioissa. Nämä toimijat hallitsevat C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) vaatimukset ja sertifiointiprosessit sekä tarjoavat paremmat mahdollisuudet määritellä kansallisia pelisääntöjä rekisteröintiin. Edellä mainitut hyödyt korostuvat esimerkiksi tilanteessa, jossa yksi kansallinen viranomaistaho, kuten toimivaltainen viranomainen, koordinoi C-ITS-yksiköille annettavia palvelukohtaisia lupia. Myönnettäessä palvelukohtaisia lupia voidaan varmistaa, että luvan hakijalla on tai että hakija saa käyttäjäoikeudet kansalliseen juurivarmennepalveluun. Hakija ohjataan toteuttamaan uusien C-ITS-yksiköiden rekisteröinti tähän palveluun. Erityisesti valtiolliseen käyttöön tarkoitettujen C-ITS-yksiköiden käyttöönotossa tämä hyöty näkyy selkeästi. Toimivaltaiselta viranomaiselta vaadittu yksiköiden käytön valtuutus voidaan yhdistää varmenteiden hankintaan kansallisesta keskitetystä palvelusta. Vaihtoehtoisena toimintamallina esitellyn toimijakohtaisen mallin vahvuuksien on tunnistettu liittyvän isoihin toimijoihin, jotka haluavat kehittää varmenteiden käyttöä ja räätälöidä varmenteiden hallintaa palvelutoimittajan kanssa yhdessä. Esimerkkeinä näistä ovat mm. ajoneuvoteollisuuden toimijat sekä laajoja liikenneympäristöjä operoivat ja hallinnoivat tahot.

Tiedonvaihtopalvelimen toteutus

Tiedonvaihtopalvelimeen liittyviä vaatimuksia on käsitelty tämän selvitystyön luvussa 7. Luku sisälsi myös ratkaisun erilaisten toteutusvaihtoehtojen punnitsemista. Vaihtoehtona tunnistettiin ratkaisun täysin itsenäinen toteutus, itsenäinen toteutus avoimen lähdekoodin avustuksella, avoimen lähdekoodin yhteisöllinen kehittäminen tai tuotehankinta.

Kehitysvaihtoehdon valinnassa on syytä ottaa erityisesti huomioon kehitettävän järjestelmään liittyvät valmiiksi olemassa olevat vaatimukset. Jos ratkaisu on vahvasti räätälöitävä täysin omiin tarpeisiin, suosii tämä piirre vahvasti räätälöidyn toteutuksen valintaa. Vahvasti toimialan standardien tai sääntelyn perusteella määritelty tuote taas mahdollistaa paremmin tuotepohjaisen hankinnan. Tämän kaltaisissa tilanteissa markkinoille myös yleensä syntyy enemmän tuotetarjontaa, kun useammilla asiakkailla on sama tarve. Näin ollen tiedonvaihtopalvelimen toteutuksessa on paljon yhtäläisyyksiä C-ITS-keskusyksikön toteutukseen.

C-Roads on määritellyt hyvin tiedonvaihtopalvelimen ominaisuuksiin liittyviä vaatimuksia. Sen keskeisimmät toiminnot ja käytettävät rajapinnat on määritelty C-Roads-spesifikaatiossa C-ITS IP Based Interface Profile (2024). Tämä tausta antaa hyvät edellytykset myös tuotepohjaisen ratkaisun harkinnalle (sillä edellytyksellä, että tuotteita syntyy eurooppalaiseen markkinaan).

Avoimen lähdekoodin hyödyntäminen on myös varteenotettava ratkaisu. Tämä toteutuslinja sisältää kaksi vaihtoehtoa. Yhtenä vaihtoehtona on olemassa olevan avoimen lähdekoodin hyödyntäminen omassa räätälöidyssä kehitysprojektissa. Tämän mallin tuottamat hyödyt näkyvät erityisesti nopeutuneessa kehitystyössä, kun avoin koodi tuottaa kehitykselle hyvän pohjan. Toisaalta merkittävä määrä valmista ohjelmistokoodia oman räätälöidyn ratkaisun pohjalle sisältää myös riskejä. Näistä keskeisimmät ovat haasteet kyseisen koodin laadukkaaseen hyödyntämiseen (hyödynnettävä koodipohja ei ole kehittäjille tuttu), ja mahdollisissa ongelmatilanteissa haastava vianmääritys.

Toisena vaihtoehtona on avoimen lähdekoodin kehittäminen yhteisöllisesti. Tämä malli sisältää avoimen lähdekoodin yhteisöön liittymisen tai yhteisön perustamisen (esim. pohjoismainen yhteisö), joka toteuttaa yhteiset linjaukset ratkaisun kehitykselle, sopii rahoitusmalleista ja luo tekemiselle hallinnollisen pohjan. Keskeisinä hyötyinä tässä mallissa tunnistetaan taloudellinen riskinjako, jonka seurauksena ”samalla rahalla saadaan enemmän”, ja mahdollisesti nopeutunut kehitystyö, kun resursseja on enemmän käytössä. Riskinä ovat erityisesti raskas yhteisön perustamisvaihe ja mahdolliset erimielisyydet ratkaisun kehittämisen suunnista ja kehityssuuntien priorisoinnista.

Yleisesti ottaen tiedonvaihtopalvelimen kehittämisestä voidaan todeta, että se ei kansallisen C-ITS-järjestelmän kehittämisen kannalta ole aikataulullisesti kiireisin tehtävä. Kansallinen C-ITS-järjestelmä saadaan käyntiin esimerkiksi yhden C-ITS-keskusyksikön ja loppukäyttäjille mobiilisovelluksilla tarjottavien palveluiden avulla. Kun järjestelmä kehittyy ja syntyy mahdollisesti useampia kansallisia, kaupunkikohtaisia tai yksityisten toimijoiden C-ITS-keskusyksiköitä ja mahdollinen tarve maiden välisiin yhteyksiin kasvaa, tiedonvaihtopalvelimelle syntyy keskeinen rooli kaikkien näiden elementtien yhdistäjänä. Toiminnan alkuvaiheessa voisi soveltuva vaihtoehto olla myös sellainen, jossa Suomessa oleva C-ITS-keskusyksikkö liitetään jossakin muussa EU-maassa sijaitsevaan tiedonvaihtopalvelimeen. Koska oletuksena on, että alkuvaiheessa C-ITS-keskusyksiköitä on Suomessa käytössä vain yksi, niin viestien löydettävyys todennäköisesti parantuisi jo merkittävästi siinä vaihtoehdossa, jossa Suomen C-ITS-keskusyksikkö olisi liitetty jossakin Suomen lähialueella olevaan tiedonvaihtopalvelimeen.

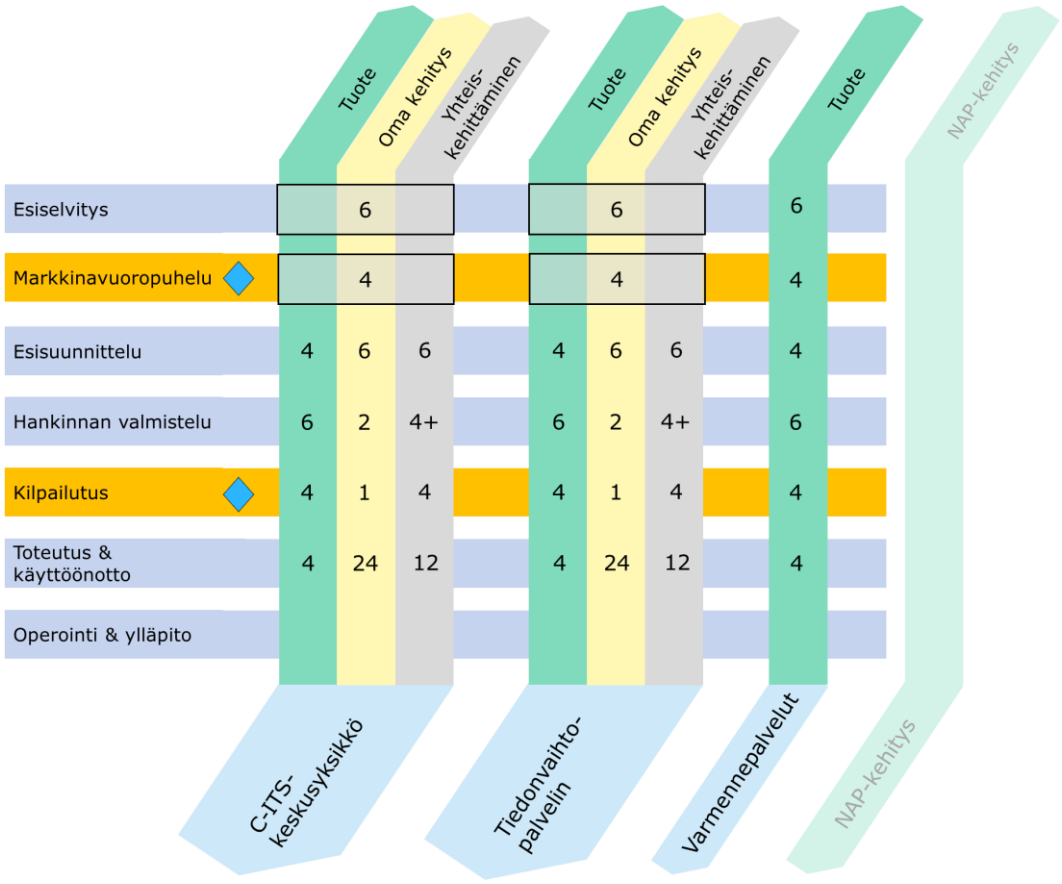
Tiedonvaihtopalvelimen toteuttamiseen liittyy paljon vaihtoehtoja, minkä vuoksi sen toteuttamisen suunnittelu kannattaa aloittaa välittömästi. Tämän tulisi sisältää neuvotteluja mahdollisten yhteiskehityskumppanien kanssa (onko halukkuutta

sekä samoja tahtotiloja) sekä olemassa olevien avoimen koodin vaihtoehtojen selvitystöitä (vrt. Norjan avoin ratkaisu). Samalla tulisi aloittaa kaupallisten ratkaisujen selvitystyö, jota voisi myös vahvistaa esimerkiksi kansallisella markkinavuoropuhelulla.

Organisoituminen

C-ITS-järjestelmien edistäminen ja kehittäminen on yleisesti ollut hallinnollinen ongelma siinä mielessä, ettei sitä ole vastuutettu selkeästi. Asioita on edistetty lähinnä yksittäisten selvitystöiden sekä pienimuotoisten kokeiluiden avulla. Näiden haasteiden ratkomiseksi sekä edellä esiteltyjen toimenpiteiden toteuttamiseksi suositellaan C-ITS-kehityksen ja käyttöönoton koordinointiryhmän perustamista. Ryhmälle suunniteltuja konkreettisia tehtäviä ovat kuvan 21 mukaiset toimet C-ITS-järjestelmän osakokonaisuuksien käyttöönoton edistämiseksi. Kansallisen yhteyspisteen (NAP) kehittäminen on huomioitu yhtenä koordinointiryhmän työhön liittyvänä toimena, mutta se on eriytetty muusta kehityksestä, koska kansallisen yhteyspisteen rooli on C-ITS-kehitystä laajempi kokonaisuus. Koordinointiryhmän keskeinen tavoite on C-ITS-toteutuksen edistäminen kokonaisvaltaisesti ja pitkäjänteisesti, ei pelkästään hanke tai selvitys kerrallaan. Koordinointiryhmän työhön liittyy oleellisesti myös C-ITS-palveluiden ja toteutuksen vaikutusarviointi.

Viranomaisten rooleja C-ITS-toteutuksessa on tutkittu aiemmassa Traficomin julkaisemassa selvityksessä (Kotilainen et al. 2023), ja kyseisessä raportissa ehdotetun roolijaon mukaisesti C-ITS-toimivaltaisen viranomaisen sekä palvelukohtaisten lupien myöntäjän roolia on ehdotettu Traficomille, jolloin on luontaista, että myös varmennepalveluiden hankinta olisi Traficomin vastuulla. Molemmat edellä mainituista ovat uusia ehdotettuja rooleja. Kansallisen C-ITS-keskusyksikön operoijan rooliin on samassa raportissa ehdotettu liikenteenohjausyhtiö Fintrafficia, joten on luontaista, että sama organisaatio olisi vastuussa C-ITS-keskusyksikön hankinnasta tai kehityksestä. Myös keskusyksikköoperaattorin rooli on uusi. On luontevaa, että C-ITS-keskusyksiköstä vastaava taho on vastuussa myös tiedonvaihtopalvelimen kehitystyöstä tai hankinnasta. Fintraffic operoi nykyisellään kansallista yhteyspistettä Väyläviraston toimeksiannosta, joten kansallisen yhteyspisteen kehityksessä on luontevaa jakaa vastuu esimerkiksi näiden toimijoiden kesken. Tärkeitä organisaatioita toteutuksen kannalta ovat myös Väylävirasto ja kunnat, sillä heillä on keskeinen rooli tie- ja katuverkon kehityksessä, ylläpidossa sekä tietojen hallinnoinnissa. Edellä mainitut organisaatiot muodostavat C-ITS-kehityksen ja käyttöönoton koordinointiryhmän ytimen. Mahdollinen ulkopuolinen apu tällaisen ryhmän toiminnan koordinoimiseen voi olla perusteltua.



Kuva 21. C-ITS-kehityksen ja käyttöönoton koordinointiryhmän konkreettiset toimet.

Ryhmän toimintakausi voi olla aluksi esimerkiksi määräaikainen, jolloin sen tehtävänä on edetä kuvan 21 mukaisissa toimissa markkinavuoropuhelu- tai kilpailutusvaiheeseen saakka.

Kuvassa esitetyt numerot viittaavat kuukausien lukumäärään, joita kyseisen vaiheen arvioidaan kestävän. Eri toteutusvaihtoehtoja koskevan *esiselvitysvaiheen* tulisi olla mahdollisimman neutraali. Saatavilla olevien kaupallisten toteutusten tilannetta tulisi selvittää markkinakartoituksen tai markkinavuoropuhelun avulla. Edellytyksiä omaan kehitystyöhön ja yhteiskehittämiseen tulisi selvittää mm. selvittämällä saatavilla olevia avoimen lähdekoodin ohjelmistoja ja ohjelmistokomponentteja ja kartoittamalla potentiaalisia yhteistyökumppaneita yhteiskehittämiseen.

Markkinavuoropuhelu on ensimmäinen luontainen päätöskohta, jossa tehdä esiselvitysten tuloksiin pohjautuva päätös siitä, halutaanko C-ITS-toteutusta edistää. Mikäli toteutuksessa päätetään edetä, on syytä aloittaa valitun toteutusmallin *esisuunnittelu* sekä *hankinnan valmistelu*. Esisuunnitteluvaihe on tuotepohjaisessa ratkaisussa oletettavasti hieman lyhyempi, sillä olemassa olevan tuotteen ominaisuudet ja toiminnallisuudet asettavat tietyt raamit. Hankinnan valmisteluvaiheessa tuotepohjaisen ratkaisun suhteen on kuitenkin tehtävä tarkempia määrityksiä, kuten myös yhteiskehittämismallissa on sovittava useista kokonaisuuksista, joita ovat esimerkiksi hallinnolliset asiat, suuntaviivat kehitystyölle sekä kaupallinen strategia. Esisuunnittelu ja hankinnan valmistelu tähtäävät kilpailutuksen toteuttamiseen.

Kilpailutus on toinen luontainen päätöksentekopiste prosessissa, jossa markkinoilta pyritään löytämään asetetut vähimmäisvaatimukset täyttävä ja hinta-laatusuhteeltaan kokonaistaloudellisesti edullisimman ratkaisun tarjoava toimittaja. Mikäli kilpailutus johtaa onnistuneeseen hankintaan, voidaan edetä *toteutus ja käyttöönotto* -vaiheeseen. Kuvan 21 mukaisesti nähdään, että vaikka oman kehityksen osalta kehitystyö on helppo ja nopea käynnistää esimerkiksi puitejärjestelysopimusten avulla, niin *toteutus ja käyttöönotto* -vaiheen arvioidaan vievän tuotepohjaista ratkaisua huomattavasti enemmän aikaa. Yhteiskehittämismallissa tätä vaihetta voi nopeuttaa se, että kumppanimaat ovat esimerkiksi jo pidemmällä kehittämisprosessissa. Onnistuneen käyttöönoton jälkeen voidaan siirtyä *operointi ja ylläpito* -vaiheeseen, jolloin toiminta muuttuu jatkuvaluonteiseksi. Koordinointiryhmän työn jatkaminen on kuitenkin edelleen perusteltua uusien C-ITS-palveluiden tai esimerkiksi kuntakohtaisten C-ITS-keskusyksiköiden kehityksen näkökulmasta. Mukaan työhön on syytä sisällyttää myös varsinaisia C-ITS-palveluntarjoajia, joiden kanssa vuoropuhelua edistetään. C-ITS-keskusyksikön sekä tiedonvaihtopalvelimen toteutus ovat samankaltaisia prosesseja, mutta varmennepalveluiden käyttöönoton suhteen markkinatilanne kaupallisesti saatavilla olevien tuotteiden suhteen on vahvempi ja puoltaa kaupallisen toimijan palvelun hankintaa.

On myös hyvä huomioida, että kuvassa esitetty *toteutus ja käyttöönotto* -vaihe voi todellisuudessa jakautua useampiin vaiheisiin, joista ensimmäisessä tavoitteena voi olla esimerkiksi rajoitetumpi kansallinen toteutus ja aloitus "pienimmällä toimivalla tuotteella" (minimum viable product). Seuraavissa vaiheissa tavoitteena voisi olla toiminnallisuuksien laajentaminen vähitellen liittämällä C-ITS-keskusyksikkö Euroopan laajuiseen tiedonvaihtopalvelinten verkostoon ja mahdollistaa näin C-ITS-keskusyksikön viestien jakaminen Euroopan laajuisesti. Alkuvaiheessa toteutettavia palveluita on myös syytä tarkastella yksityisyyden suojan näkökulmasta. Niin kauan kuin EU-tasoista käsittelyperustetta ja vakiintunutta oikeuskäytäntöä ei ole, toteutuksessa on turvallisinta pitäytyä palveluissa, jotka eivät sisällä henkilötietoja. Näitä ovat I2V-tyyppiset (Infrastructure-to-Vehicle) C-ITS-palvelut (esimerkiksi tietöihin tai keliolosuhteisiin liittyvät varoituspalvelut). Yksityisyyden suojan näkökulmasta luvussa 8.4 käsitellään tarkemmin kahden ensisijaisen C-ITS-palvelun toteutusta. Tämä työ ei kuitenkaan sisällä kattavampaa palvelukohtaista tarkastelua kansallisesta C-ITS-toteutuksen toimeenpanosta. Tässä selvityksessä on tunnistettu, että hyvät ja toimivat käytännöt voivat osaltaan auttaa korvaamaan yksityisyyden suojaan liittyvän lainsäädännön puutteita. Yhteistyö voi auttaa selkeyttämään C-ITS-palveluiden turvallisen ja tehokkaan toteuttamisen kannalta välttämättömiä vastuita ja toimintamalleja. Ehdotetun C-ITS-kehityksen ja käyttöönoton koordinointiryhmän perustamisen on tarkoitus osaltaan vastata tähän tarpeeseen.

Toteutuksessa on syytä huomioida myös C-ITS-turvallisuus- ja varmennepolitiikkojen suositukset C-ITS-yksikköoperaattoreille, joiden mukaisesti C-ITS-yksiköitä suositellaan otettavan käyttöön vaiheittain. Tällä viitataan C-ITS-turvatunnusten hallintajärjestelmään (EU CCMS), joka sisältää tasojen L0-L2 mukaiset toimintamallit, kuten on tarkemmin luvun 4.2.4 yhteydessä esitetty. Tiiviisti näiden tasojen eroina on se, että L2-taso vastaa tuotantokäyttöä, L1-taso on tarkoitettu väliaikaiseen tuotantokäyttöön ja tasolle L2 siirtymisen edellytysten luomiseen ja L0-taso on tarkoitettu pilotointiin. Teknologiaan liittyvä alkuvaiheen kehitystyö voidaan toteuttaa L0-tasolla. Tasoilla voidaan sen jälkeen nousta ylöspäin C-ITS-yksiköiden vaatimustenmukaisuutta ja organisaation toimintaa koskevien osa-alueiden kehittyessä. Toki on hyvä huomioida, että varsinaisia tuotantopalveluita ei

voida alkaa tuottamaan pysyvästi, ennen kuin toiminta on L2-tason mukaista. Tämän kaltainen vaiheittainen etenemispolku ei ole pakollinen, mutta suosituksena on huomioida tämä.

Suosituksena on myös, että perustettava koordinaatiotyöryhmä osallistuu aktiivisesti toimintaan keskeisillä foorumeilla ja että erityisesti pitkän kantaman tiedonsiirtoon perustuvien ratkaisujen määrittelyjen kehittymistä seurataan vahvasti. Keskeisiä tunnistettuja foorumeita ovat jo edellisessä luvussa laatumäärittelyjen yhteydessä mainitut C-Roadsin eri työryhmät (esim. Hybrid Communication -työryhmä), Data for Road Safety -ekosysteemi sekä EU:n tienpitäjistä ja operaattoreista koostuva RTTI-työryhmä (RTTI Task force). Kansallisen C-ITS-ekosysteemin määrittely- ja kehitystyön edetessä voidaan foorumeille tuoda myös konkreettisia esitysehdotuksia toteutusmalleiksi ja näin varmistaa kansallisen toteutuksen yhteentoimivuus Euroopan laajuisen sääntelykehikon kanssa.

Toimenpiteiden edistämiseen liittyvät riskit

Kansallisen C-ITS-toteutuksen edistämiseen liittyviä toimenpiteitä voidaan tarkastella myös riskiluokittelun näkökulmasta jakamalla toimet matalan, keskitason sekä korkean riskin toimenpiteisiin taulukon 19 mukaisesti. Taulukon riskeillä tarkoitetaan tässä yhteydessä riskejä hyöty-kustannusnäkökulmasta, eli käytännössä varmuutta, jolla C-ITS-toteutukseen investoidut eurot ja resurssit tuottavat yhteiskuntataloudellisia hyötyjä. Taulukon mukaiseen riskiluokkaan vaikuttaa siis se, miten paljon toimenpide on räätälöity tiettyyn C-ITS-toteutusmalliin tai millaisia kustannusvaikutuksia se aiheuttaa. Kuten työn rajauksissa (luku 1.2) on esitetty, ei tässä työssä ole toteutettu varsinaista C-ITS-palveluiden vaikutusten arviointia, vaan taulukon mukaisella tarkastelulla pyritään ennemminkin havainnollistamaan asioita, joihin kansallisessa toteutusmallissa on syytä kiinnittää huomiota.

Taulukko 19. Toimenpiteiden riskiluokittelu

Toimenpide	Riskiluokka	Kuvaus
Varmenne-palveluiden hankinta	Keskitaso	Varmennepalvelu tulee hankkia kaikissa eri C-ITS-toteutusvaihtoehdoissa, riippumatta siitä millaisilla C-ITS-yksiköillä palvelut toteutetaan. Tämä pienentää varmennepalveluiden hankintaan kohdistuvaa riskiä. Riskinä on, että mikäli C-ITS-palveluita ei päädyttäisikään toteuttamaan, varmennepalvelut olisivat tarpeettomia. Tämä korostaa sitä, että kaikissa C-ITS-järjestelmän osien toteutuksessa on hyvä edetä yhtäaikaisesti.
C-ITS-keskus-yksikön toteutus	Korkea	C-ITS-keskusyksikön sekä tiedonvaihtopalvelimen toteutukseen liittyvät riskit ovat korkeat, sillä näissä molemmissa osakokonaisuuksissa on mahdollista edetä useamman vaihtoehtoisen toteutusmallin (kaupallinen hankinta, oma kehitys/räätälöity toteutus tai avoimeen lähdekoodiin perustuva yhteiskehittäminen) mukaisesti. Investoinnit ja oma resursointitarve vaihtelevat toteutusmallin mukaan, mutta ovat joka vaihtoehdossa merkittäviä. Riskiä voidaan hallita asteittaisella etenemisellä ja toteutuksella, jolloin suuria investointeja ei tehdä kerralla vaan kehityksen edetessä ja tiedon karttuessa.
Tiedonvaihto-palvelimen toteutus	Korkea	
Kansallisen yhteyspisteen kehittäminen	Matala	SRTI- ja RTTI-tietojen laajamittainen kerääminen kansalliseen yhteyspisteeseen ja yhteyspisteen kehittäminen palvelemaan C-ITS-viestien muodostamista on tunnistettu matalan riskin toimena. Tietotyyppien keräämiseen on EU-direktiivin asettama velvoite, joten näitä toimia on edistettävä joka tapauksessa. C-ITS-viestien muodostamiseen kansallisen yhteyspisteen avulla riittää yksinkertaisimmillaan rajapintakehitys.

Vaikka C-ITS-palvelutoteutuksen arkkitehtuurin edistämiseen kohdistuu taulukon 19 mukaisia riskejä, niin on syytä huomioida, että C-ITS-toteutukseen liittyvien toimien tekemättä jättäminen ei myöskään ole täysin riskitöntä. Mikäli kansallista C-ITS-toteutusta ei edistetä, vaikutuskeinot keskeisillä foorumeilla ovat rajallisemmat, kun ehdotuksia ei voida pohjustaa toimiviksi todennetuilla toteutusmalleilla. Vaarana voi myös olla, että keskeisiin Euroopan laajuisiin C-ITS-kehitystä ohjaaviin dokumentteihin sisällytetään kansallisesta näkökulmasta epäsuotuisia määrittelyjä ja vaatimuksia. Reaktiivinen rooli C-ITS-kehityksen suhteen viivästyttää palveluiden kansallista käyttöönottoa, jolloin myös C-ITS-palveluiden odotetut positiiviset vaikutukset liikennejärjestelmän turvallisuuteen, ympäristöystävällisyyteen tai tehokkuuteen viivästyvät. Kuten tämän luvun yhteydessä on osoitettu, aikajänne C-ITS-järjestelmän osakokonaisuuksien toteutukseen liittyvän tarkemman esiselvitystyön aloittamisesta operointi ja ylläpito -vaiheeseen on todennäköisesti useita vuosia.

12 Tulosten arviointi

Tässä raportissa esitettiin ehdotus C-ITS-palveluiden käyttöönoton valmiuksien edistämiseksi huomioiden C-ITS-keskusyksikön toteutus ja operointi EU:n C-ITS-turvallisuus- ja varmennepolitiikkojen mukaisesti, C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) käyttöönotto sekä tiedonvaihtopalvelimeen kohdistuvat vaatimukset ja sen käyttöönotto Suomessa. Ehdotuksessa C-ITS-palveluiden käyttöönoton valmiuksien edistämiseksi Suomen oloissa huomioitiin lisäksi yksityisyyden suojaan liittyvät näkökulmat. Tässä luvussa arvioidaan työssä saatujen tulosten luotettavuutta sekä työn tuloksiin liittyviä rajoitteita ja epävarmuustekijöitä.

Työn tulosten luotettavuuteen vaikuttaa yleisesti C-ITS-teknologian kypsyysaste, eli toisin sanoen C-ITS-palveluita koskevien spesifikaatioiden ja määrittelyjen keskeneräisyys sekä niiden soveltamisesta saatujen kokemusten vähäisyys. C-Roads Platform -yhteistyöryhmän ja EU:n C-ITS-turvallisuus- ja varmennepolitiikkojen mukaisesti toimivia palvelutoteutuksia on lukumäärällisesti vasta vähän. Työssä ei tunnistettu C-ITS-turvatunnusten hallintajärjestelmän (EU CCMS) tason L2 (tuotantokäyttöä vastaava taso) mukaisia olemassa olevia pitkän kantaman tiedonsiirtoratkaisuun perustuvia toteutuksia. Pitkän kantaman tiedonsiirtoon perustuvissa toteutuksissa C-ITS-keskusyksiköiden turvaprofiilien puute sekä HSM-moduulien käytön vaatimukset konesaliympäristössä ovat esimerkkejä keskeisistä määriteltävistä asioista.

C-ITS-palveluita koskeva lainsäädäntö on myös osin aukollinen, sillä esimerkiksi henkilötietojen käsittelyä C-ITS-palveluissa koskevat perusteet eivät ole yksiselitteisesti määriteltyjä. Lainsäädännölliseen kehykseen liittyen Suomella on rajallinen kyvykkyys tehdä ratkaisuja, sillä moni asia on EU:n päätäntävallassa eikä kansallista lainsäädäntöä kannata välttämättä tehdä ennen EU-tason linjauksia, jotta ratkaisujen Euroopan laajuisesta yhteentoimivuudesta voidaan varmistua. Näin ollen myös palveluita koskevan sääntelyn tulevaan kehitykseen liittyy epävarmuuksia, sillä EU-tasoisen sääntelyn kehitys on vaikeasti ennakoitavissa. Raportissa on esitetty tärkeänä jatkotoimena erilaisiin sääntelykehyksiin vaikuttaminen keskeisten työryhmien kautta.

Työssä saatujen tulosten merkittävyyttä lisäävä tekijä on erityisesti tulosten uutuusarvo, sillä C-ITS-järjestelmiin liittyvien spesifikaatioiden (ml. EU CCMS ja C-Roads-profiilispesifikaatiot) soveltamisesta on toistaiseksi vain rajallisesti kokemusta. Uutuusarvoa ja tulosten merkittävyyttä C-ITS-palveluiden toteutuksen ja käyttöönoton suunnittelussa lisää myös se, ettei pitkän kantaman tiedonsiirtoratkaisuun perustuvia ja tason L2-vaatimukset täyttäviä palvelutoteutuksia toistaiseksi tunneta. Pilotoinnista käytössä oleviin tuotantovaiheen palveluihin siirtyminen on ajankohtainen teema C-ITS-järjestelmien kehitystyössä, ja tätä kehitystyötä tämän raportin tulokset erityisesti tukevat.

Tämän selvitystyön lopputuloksena on ehdotus kansallisesta C-ITS-järjestelmän toteutusmallista. Keskeisenä tutkimuskysymyksenä oli tunnistaa olemassa olevien spesifikaatioiden mahdollisesti sisältämiä esteitä C-ITS-palveluiden käyttöönottoon Suomessa. Käyttöönottoa kokonaan estäviä syitä ei työn aikana tullut esiin. Käyttöönottoa voi jossakin määrin kuitenkin vaikeuttaa yksikköoperaattoreihin kohdistuvat tietoturvallisuuden hallintajärjestelmän käyttöönottoon liittyvät vaatimukset. Standardin ISO 27001 mukaisen sertifioidun tietoturvallisuuden

hallintajärjestelmän toteuttaminen on merkittävä kustannus uudelle C-ITS-yksiköitä käyttöön ottavalle toimijalle. Raportissa esitettyjen arvioiden mukaan käyttöönoton kustannusten alaraja on todennäköisesti joitakin kymmeniä tuhansia euroja jatkuvien vuosittaisten suorien kustannusten ja välillisten kustannusvaikutusten kasvaessa jopa suuremmiksi. Tämä mahdollisesti rajaa pienimmät toimijat kokonaan pois C-ITS-yksiköiden operaattoreiden joukosta (esimerkiksi joukkoliikenteen liikennöitsijät, hinauspalvelun tarjoajat ja pienemmät kunnat sekä pienemmät ohjelmistotoimijat) tai saattaa tehdä käyttöönoton kustannuksista odotettavissa olevia hyötyjä suuremmat myös isommille toimijoille. Tämä koskee erityisesti toimijoita, jotka jäävät NIS-direktiiveissä määriteltyjen yritysten kokorajojen alapuolelle eivätkä muustakaan syystä ole NIS-direktiivien velvoitteiden piirissä, mutta joihin vaatimukset kohdistuvat välillisesti esimerkiksi kilpailutusten myötä. Jatkotutkimuskysymyksenä on syytä harkita, voidaanko NIS1- ja NIS2-direktiiveihin perustuvassa vaihtoehdossa tarjota kustannuksiltaan edullisempi polku tai valmiit kansallisen tason ohjeet näille toimijoille, ja mitkä toimijat voisivat potentiaalisesti olla tämän vaihtoehdon piirissä.

Vaikka C-ITS-järjestelmän käyttöönotolle ei tunnistettu varsinaisia esteitä, ei keskusyksikön tai tiedonvaihtopalvelimen toteutusmalliksi voitu antaa yksiselitteistä ehdotusta, koska tämä vaatii tarkemman esitettyjä vaihtoehtoja selkeyttävän esiselvityksen ja markkinakartoituksen. Raportin tulosten perusteella ei voida myöskään yksiselitteisesti arvioida, kannattaako C-ITS-toteutusta edistää, sillä toteutuksen yhteiskuntataloudellisia hyötyjä ei ole arvioitu. Raportti kuitenkin esittää C-ITS-palveluita toteuttavan järjestelmän mahdolliseen käyttöönottoon liittyvän toimeenpanosuunnitelman, jonka osana tällaisen selvityksen tekemistä suositellaan. Raportti antaa hyvät edellytykset ja lähtökohdat jatkaa systemaattisesti mahdollista C-ITS-järjestelmien käyttöönoton edistämistä Suomessa.

13 Lähdeluettelo

Almaviva haastattelu, 2024, Teams, 21.10.2024, 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. Saatavilla: https://ec.europa.eu/newsroom/article29/items/610171/en (Viitattu: 20.2.2025).

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. Verkkosivu. Saatavilla www-osoitteesta: https://www.car-2-car.org/about-c-its#c1001 (Viitattu: 18.2.2025).

CCAM Partnership, 2023, Strategic Research and Innovation Agenda (SRIA). Saatavilla www-osoitteesta: https://www.ccam.eu/wp-content/uploads/2023/11/CCAM-SRIA-Update-2023.pdf (Viitattu 12.2.2025).

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. Saatavilla www-osoitteesta: 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, 9.3.2023, 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. Saatavilla www-osoitteesta: https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0._20230916.pdf

COSS ry haastattelu, 2024, Teams, 25.9.2024, Aihe: Avoimen lähdekoodin yhteisöjen hyödyntäminen julkishallinnon ohjelmistohankkeissa, 25.9.2024.

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. Saatavilla www-osoitteesta: 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, 14.12.2023.

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. www-osoite: 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. Saatavilla www-osoitteesta: https://www.dataforroadsafety.eu/images/Documenten/20210706_Privacy_Statement._DFRS_ecosystem.pdf (Viitattu: 24.2.2025).

De Luca, S., 2024. The path to 6G. European Parliamentary Research Service Briefing. Saatavilla www-osoitteesta: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757633/EPRS_BRI%282024%29757633_EN.pdf

ETSI TS 102 941, 2022. Intelligent Transport Systems (ITS); Trust and Privacy Management, v.2.2.1. ETSI. Saatavilla www-osoitteesta: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/02.02.01_60/ts_102941v020201p.pdf (Viitattu: 23.2.2025).

ETSI TS 103 097, 2022. Intelligent Transport Systems (ITS); Security header and certificate formats, v.2.1.1. ETSI. Saatavilla www-osoitteesta: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/02.01.01_60/ts_103097v020101p.pdf (Viitattu: 23.2.2025).

ETSI TS 102 940, 2021, Technical Specification "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2". Saatavilla www-osoitteesta: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf

EU 2010/40/EU, 2010, Euroopan parlamentin ja neuvoston direktiivi 2010/40/EU, annettu 7 päivänä heinäkuuta 2010, tieliikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista. Saatavilla www-osoitteesta: https://eur-lex.europa.eu/eli/dir/2010/40/oj/eng

EU 2002/58, 2002, Euroopan parlamentin ja neuvoston direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi). Saatavilla www-osoitteesta: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=LEGISSUM:l24120 (Viitattu: 20.2.2025).

EU 2016/588, 2016, Komission tiedoksianto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealla, annettu 14.9.2016, "5G for Europe: An Action Plan". Saatavilla www-osoitteesta: https://digital-strategy.ec.europa.eu/en/library/communication-5g-europe-action-plan-and-accompanying-staff-working-document (Viitattu 30.12.2024).

EU 2016/679, 2016, Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (GDPR, yleinen tietosuoja-asetus). Saatavilla www-osoitteesta: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679#cpt_IV (Viitattu: 20.2.2025)

EU 2021/118, 2021, Komission tiedoksianto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealla, annettu 9.3.2021."2030 Digital Compass: the European way for the Digital Decade". Saatavilla www-osoitteesta: 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=fi

EU 2022/2557, 2022, Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557 ,annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta. Saatavilla www-osoitteesta: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

EU 2023/2661, 2023, Euroopan parlamentin ja neuvoston direktiivi (2023) 2661, annettu 30.11.2023, ”Euroopan parlamentin ja neuvoston direktiivi tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista annetun direktiivin 2010/40/EU muuttamisesta”. Saatavilla www-osoitteesta: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L_202302661

EU C/2016/766, 2016, Komission tiedoksianto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealla, annettu 30.11.2016, ”Eurooppalainen strategia vuorovaikutteisia älykkäitä liikennejärjestelmiä varten - ensimmäinen virstanpylväs matkalla kohti vuorovaikutteista, verkkoon liitettyä ja automatisoitua liikkumista”. Saatavilla www-osoitteessa: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0766&from=FR

EU C/2019/1789, 2019, Komission delegoitu asetus C(2019) 1789, annettu 13.3.2019, ”Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU täydentämistä yhteistoiminnallisten älyliikennejärjestelmien käyttöönoton ja operatiivisen käytön osalta”. Saatavilla www-osoitteessa: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282019%291789

EU C/2024/6798, 2024. Komission täytäntöönpanopäätös direktiivin 2010/40/EU työohjelman vahvistamisesta vuosiksi 2024–2028. Euroopan unionin virallinen lehti. Saatavilla www-osoitteessa 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. Saatavilla www-osoitteesta: https://commission.europa.eu/about/departments-and-executive-agencies/digital-services/open-source-software-strategy_en

Euroopan komissio, 2022, 5G Kattavuus liikennekäytävillä: 5G-käytävien infrastruktuurien yhteisrahoitukseen valittujen hankkeiden ensimmäinen aalto, Euroopan unionin virallinen verkkosivusto. Verkkosivu. Julkaistu 22. joulukuuta 2022. Saatavilla www-osoitteesta: https://digital-strategy.ec.europa.eu/fi/news/5g-coverage-along-transport-corridors-first-wave-projects-selected-co-funding-5g-corridor (viitattu 30.12.2024).

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. Hyväksytty 9. maaliskuuta 2021. Saatavilla: https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf (Viitattu: 23.2.2025).

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. Saatavilla www-osoitteesta: https://www.fcc.gov/document/fcc-adopts-c-v2x-auto-safety-spectrum-rules

Fintraffic haastattelu, 2024, Teams, 28.8.2024, 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. Saatavilla www-osoitteesta: 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. Saatavilla www-osoitteesta: https://datatracker.ietf.org/doc/html/rfc8446

Intens haastattelu, 2024, Teams, 30.10.2024, 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), Saatavilla www-osoitteesta: https://www.iso.org/standard/66924.html (maksullinen)

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), Saatavilla www-osoitteesta: https://www.iso.org/standard/72891.html (maksullinen)

ISO/IEC 19464, 2014, ISO/IEC 19464:2014 Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification, Published (Edition 1, 2014), maksullinen standardi.

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". Traficomin tutkimuksia ja selvityksiä 11/2024. Saatavilla www-osoitteesta: 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". Traficomin tutkimuksia ja selvityksiä 23/2023. Saatavilla www-osoitteesta: 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". Traficomin tutkimuksia ja selvityksiä 12/2024. Saatavilla www-osoitteesta: 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". Traficomin tutkimuksia ja selvityksiä 20/2024. Saatavilla www-osoitteesta: https://www.traficom.fi/sites/default/files/media/publication/RTTI-asetus%20raportti%2020_2024.pdf

Laki sähköisen viestinnän palveluista 917/2014. Saatavilla www-osoitteesta: https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#O6L17P138 (Viitattu: 20.2.2025).

Liikenne- ja viestintäministeriö, 2024, Kestävää kasvua, hyvinvointia sekä turvallisuutta tiedolla ja tulevaisuuden yhteyksillä: Liikenne- ja viestintäministeriön hallinnonalan konsernistrategia. Liikenne- ja viestintäministeriön julkaisuja 2024:3. Saatavilla www-osoitteesta: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165418/LVM_2024_3.pdf?sequence=1&isAllowed=y

Linux Foundation, 2024, Open Source Guides - Setting an Open Source Strategy. Verkkosivu. Saatavilla www-osoitteesta: https://www.linuxfoundation.org/resources/open-source-guides/setting-an-open-source-strategy (Viitattu 12.2.2025).

LVM/2021/137, 2021, Valtioneuvoston periaatepäätös liikenteen automaation edistämisestä. Saatavilla www-osoitteesta: 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. Raporttiluonnos. Saatavilla: https://www.cedr.eu/docs/view/671a142d82dd7-en (Viitattu: 21.2.2025)

Menezes, A., van Oorschot, P., Vanstone, S., 1996, The Handbook of Applied Cryptography. Saatavilla www-osoitteessa: https://cacr.uwaterloo.ca/hac/about/chap1.pdf

Microsec ja Commsignia haastattelu, 2024, Teams, 29.8.2024, 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”. Liikenne- ja viestintäministeriön julkaisuja 2021:28. Saatavilla www-osoitteesta: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163629/LVM_2021_28.pdf?sequence=1&isAllowed=y

Monotch haastattelu, 2024, Teams, 21.8.2024, 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, Saatavilla www-osoitteesta: https://www.amqp.org/resources/download

Rekola, M., Kolinen, L., Asikainen, E., Heliste, L., Immonen, E., Starck, M., Ahokas, M., Suomento, J., Johansson, S., 2022. ” Liikenneturvallisuusstrategia 2022–2026”. Liikenne- ja viestintäministeriön julkaisuja 2022:3. Saatavilla www-osoitteesta: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163951/LVM_2022_3.pdf?sequence=1&isAllowed=y

Swarco haastattelu, 2024, Teams, 22.10.2024, Subject:” The deployment of the EU CCMS compatible C-ITS ecosystem in Finland and the role of C-ITS units”.

TEN-TEC EU-maiden C-ITS-keskusyksiköt, 2025, European Commission TENtec Version 6.1.0 (Filter: C-ITS Stations & Networks). Verkkosivu. Saatavilla www-osoitteessa: https://webgate.ec.europa.eu/tentec-maps/web/public/screen/home (Viitattu 24.2.2025).

Teskalabs haastattelu, 2024, Teams, 5.9.2024, 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-välilehti). Verkkosivu. Saatavilla www-osoitteesta: https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms (Viitattu 24.2.2025).

Tietosuojalaki 1050/2018, 2018. Saatavilla www-osoitteesta: https://finlex.fi/fi/laki/ajantasa/2018/20181050 (Viitattu: 20.2.2025).

Tietosuojavaltuutetun toimisto (n.d.) *Arvioi riskit*. Verkkosivu. Saatavilla www-osoitteesta: https://tietosuoja.fi/arvioi-riskit (Viitattu: 20.2.2025).

Tietosuojavaltuutetun toimisto (n.d.) *Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle*. Verkkosivu. Saatavilla www-osoitteesta: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle (Viitattu: 20.2.2025).

Tietosuojavaltuutetun toimisto (n.d.) *Käsittelyperusteet*. Verkkosivu. Saatavilla www-osoitteesta: https://tietosuoja.fi/kasittelyperusteet (Viitattu: 20.2.2025).

Tietosuojavaltuutetun toimisto (n.d.) *Pseudonymisoidut ja anonymisoidut tiedot.* Verkkosivu. Saatavilla www-osoitteesta: https://tietosuoja.fi/pseudonymisointi-anonymisointi (Viitattu: 20.2.2025).

Tietosuojavaltuutetun toimisto (n.d.) *Tiedonsiirtovälineitä täydentävät suojatoimet*. Verkkosivu. Saatavilla www-osoitteesta: https://tietosuoja.fi/tiedonsiirtovalineita-taydentavat-suojatoimet (Viitattu: 20.2.2025).

Tietosuojavaltuutetun toimisto (n.d.) *Tietoturvaloukkaukset*. Verkkosivu. Saatavilla www-osoitteesta: https://tietosuoja.fi/tietoturvaloukkaukset (Viitattu: 20.2.2025).

Tietosuojavaltuutetun toimisto (n.d.) *Vaikutustenarviointi*. Verkkosivu. Saatavilla www-osoitteesta: https://tietosuoja.fi/vaikutustenarviointi (Viitattu: 20.2.2025).

Traficom, 2024. Tarjouspyyntö: Liikenne- ja viestintävirasto 525852 / C-ITS-palveluiden tarve ja priorisointi Suomessa - Liikenne- ja viestintävirasto Traficom - Älyliikenteen, automaation ja liikkumispalveluiden asiantuntijapalvelut (DPS), sisäinen kilpailutus (DPS), päiväys 9.9.2024.

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. Saatavilla www-osoitteesta: https://unece.org/sites/default/files/2023-02/R155e%20%282%29.docx

Valtioneuvosto, 2023. "Vahva ja välittävä Suomi: Pääministeri Petteri Orpon hallituksen ohjelma 20.6.2023". Valtioneuvoston julkaisuja 2023:58. Saatavilla www-osoitteesta: https://julkaisut.valtioneuvosto.fi/handle/10024/165042

Valtioneuvosto, 2024. "Valtakunnallinen liikennejärjestelmäsuunnitelma vuosille 2026–2037". Valtioneuvoston julkaisuja 2024:XX. Suunnitelmaluonnos. Saatavilla www-osoitteesta: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=47f126a9-4eea-43c5-a4ba-c57137827636

Vegvesen haastattelu, 2024, Teams, 8.10.2024, 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"

Vientiklusteri, n.d. Fintraffic. Verkkosivu. Saatavilla www-osoitteesta: https://www.fintraffic.fi/fi/liikenteendataekosysteemi/vientiklusteri (Viitattu 20.1.2025).

Viswanathan, H. & Mogensen, P., 2023. Communications in the 6G Era. Espoo: Nokia Bell Labs White Paper. Saatavilla www-osoitteesta: 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. Saatavilla www-osoitteesta: 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. Saatavilla www-osoitteesta: https://doi.org/10.1186/s12544-024-00694-6

Liikenne- ja viestintävirasto Traficom
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

ISBN 978–952–311–980–2
ISSN 2669–8781 (verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto