



Univerza v Mariboru

Fakulteta za gradbeništvo,
prometno inženirstvo in arhitekturo

Tehnična specifikacija za CENTRALNI NACIONALNI OBLAK ZA C-ITS (CENTRAL C-ITS CLOUD)

Verzija 1.2: 20. 11. 2023

KAZALO

1	Referenčni normativi, sistemi in definicije	5
2	Uvod	6
2.1	Projekt C-Roads	6
2.2	Piloti DARSa	9
3	Vsebina naročila	11
3.1	Namen in cilji	11
3.2	Shema sistema	12
3.3	Storitve in scenariji.....	14
3.3.1	Storitev Prenos prometne signalizacije v vozilo (In-Vehicle Signage - IVS)	15
3.3.2	Storitev Opozorilo o nevarnih lokacijah (Hazardous Locations Notification - HLN)	15
3.3.3	Storitev Opozorilo o delih na cesti (Road Works Warning - RWW)	16
3.3.4	Storitev Semaforizirana križišča (Signalized Intersections - SI).....	17
3.3.5	Storitev Podatki o gibanju vozil (Probe Vehicle Data - PVD)	17
3.4	Centralna postaja C-ITS	17
3.4.1	Arhitektura centralne postaje C-ITS	18
3.4.2	Geolociranje.....	19
3.4.3	Varnost	19
3.5	Aktivnosti	20
4	Nefunkcionalne zahteve	21
4.1	Uporabnost	21
4.2	Razpoložljivost.....	21
4.3	Zanesljivost.....	21
4.4	Zmogljivost.....	21
4.5	Nadgradljivost.....	22
4.6	Skalabilnost	22
4.7	Varnost	22
4.8	Tehnološke zahteve	23
5	Metodološke zahteve.....	24
5.1	Vodenje projekta in poročanje na strani izvajalca	24
5.2	Metodologija razvoja in terminski načrt	24
5.3	Analiza in specifikacija zahtev	24
5.4	Implementacija rešitve	25
5.5	Namestitev rešitve	25
5.6	Testiranje in zagotavljanje kakovosti	26

5.6.1	Načrt testiranja.....	26
5.6.2	Testni scenariji in ugotovljene napake.....	26
5.6.3	Testni scenarij.....	26
5.6.4	Poročilo o testiranju	27
5.7	Uporabniška in tehnična dokumentacija.....	27
5.7.1	Programska koda.....	27
5.7.2	Tehnična dokumentacija - splošno	27
5.7.3	Tehnična dokumentacija - namestitvev	27
5.7.4	Uporabniška dokumentacija	28
5.8	Usposabljanje uporabnikov	28
6	Okvirni terminski načrt projekta	29
7	Jamčevanje in vzdrževanje	30
7.1	Jamčevanje v garancijskem obdobju:	30

1 Referenčni normativi, sistemi in definicije

S tematiko povezani referenčni normativi so:

- Direktiva 2010/40/EU Evropskega parlamenta in Sveta z dne 7. 7. 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza (<http://data.europa.eu/eli/dir/2010/40/oj>), spremenjena s Sklepom (EU) 2017/2380 Evropskega parlamenta in Sveta z dne 12. 12. 2017 o spremembi Direktive 2010/40/EU glede obdobja za sprejemanje delegiranih aktov (<http://data.europa.eu/eli/dec/2017/2380/oj>), konsolidirana dne 9. 1. 2018 (<http://data.europa.eu/eli/dir/2010/40/2018-01-09>) (v nadaljnjem besedilu: Direktiva 2010/40/EU).
- Delegirana uredba komisije (EU) 2022/670 z dne 2. 2. 2022 o dopolnitvi Direktive 2010/40/EU Evropskega parlamenta in Sveta v zvezi z opravljanjem storitev zagotavljanja prometnih informacij v realnem času po vsej EU (http://data.europa.eu/eli/reg_del/2022/670/oj).
- Novelacija Direktive 2010/40/EU je 11. 10. 2023 potrdil Evropski parlament in Svet EU in (v času priprave tega dokumenta) čaka na uradno objavo: Directive of the European parliament and of the Council amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (<https://www.consilium.europa.eu/en/press/press-releases/2023/10/23/council-adopts-new-framework-to-boost-the-roll-out-of-intelligent-transport-systems/>).
- Evropska strategija za kooperativne inteligentne prometne sisteme (C-ITS) – mejnik na poti h kooperativni, povezani in avtomatizirani mobilnosti (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766>).
- Uredba (EU) št. 1315/2013 Evropskega parlamenta in Sveta z dne 11. 12. 2013 o smernicah Unije za razvoj vseevropskega prometnega omrežja in razveljavitvi Sklepa št. 661/2010/EU ([UL L 348, 20.12.2013, str. 1](http://eur-lex.europa.eu/legal-content/EN/LEX/348/2013/str.1)), ki se nanaša na TEN-T in se uporablja v skladu s členom 5 Direktive 2010/40/EU.
- Zakon o cestah (ZCes-2), Uradni list RS, št. 132/22, 140/22 – ZSDH-1A, 29/23 in 78/23 – ZUNPEOVE, (<http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO8298&d-49687-s=0>).

2 Uvod

Inteligentni transportni sistemi (ITS) imajo za cilj izboljšati prometno varnost, učinkovitost prometa ter narediti promet skladnejši s smernicami trajnostnega razvoja. Cilji strateških okvirjev razvoja vseevropskega prometnega omrežja kot temeljne hrbtenice EU (Uredba (EU) št. 1315/2013, ki se nanaša na TEN-T in Direktivo 2010/40/EU), smernic na področju digitalne transformacije EU in celovite strategije razvoja kooperativnih ITS (Novelacija Direktive 2010/40/EU, Evropska strategija za kooperativne inteligentne prometne sisteme - C-ITS) vodijo do kooperativne, povezane in avtomatizirane mobilnosti. Sistemi C-ITS so namenjeni neposredni interakciji uporabnikov in upravljalcev prometne infrastrukture s samo prometno infrastrukturo. Akterji in infrastruktura medsebojno delijo informacije z namenom koordinacije aktivnosti na območju prometne infrastrukture. Namen omenjene strategije je vseevropska in čezmejna harmonizacija storitev C-ITS. Za implementacijo omenjene strategije je bila vzpostavljena vseevropska platforma C-Roads (<https://www.c-roads.eu/>), ki zajema 18 evropskih držav, t.i. jedrnih članic platforme ter 7 pridruženih članic. Slovenija je članica platforme od njene ustanovitve v letu 2016. Platforma je zasnovana tako, da omogoča vzporedno izvajanje razvojnih aktivnosti na nacionalnih nivojih in hkrati zagotavlja njihovo medsebojno skladnost in povezanost.

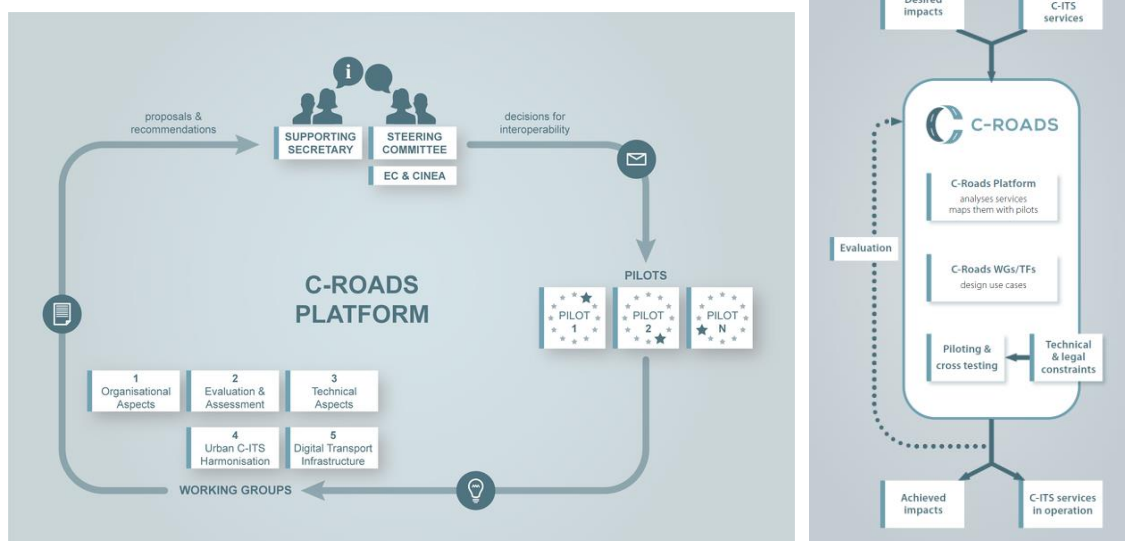
C-ITS zaobjema nabor tehnologij in aplikacij, ki omogočajo učinkovito izmenjavo podatkov med vsemi akterji, ki prihajajo v stik s transportnim sistemom, in sicer s pomočjo mobilnih tehnologij in brezžične komunikacije. Komunikacija vključuje tako izmenjavo podatkov med vozili (V2V), kot izmenjavo podatkov in sporočil med vozili in prometno infrastrukturo (V2I). Na ta način C-ITS zagotavlja lokacijsko ustrezne, pravilne in pravočasne informacije uporabnikom glede na situacijo v kateri se trenutno nahajajo. C-ITS predstavlja nadgradnjo obstoječih sistemov ITS in razširja njihovo delovanje na področjih kot so upravljanje prometa, zagotavljanje prometnih informacij v realnem času, zagotavljanje prometne varnosti in podobno.

Podlaga za aktivnosti vzpostavitve C-ITS je Direktiva 2010/40/EU, ki je podala usmeritve kaj je res treba razviti, uskladiti in vpeljati (kot npr. tehnične specifikacije, standarde, potrebne/minimalne zahteve, vmesnike, ukrepe). V skladu s 118. členom Zakona o cestah (ZCes-2) je za spremljanje razvoja in uporabe aplikacij in storitev, ter nadzor čezmejne harmonizacije in medobratovalnosti rešitev ITS in C-ITS pristojen NCUP.

V nadaljevanju je predstavljeno obstoječe stanje razvoja C-ITS v Sloveniji. Predstavljen je DARS-ov projekt C-ROADS ter izvedeni pilotni projekti v Sloveniji.

2.1 Projekt C-Roads

Platforma C-Roads je zasnovana tako, da uvajanje C-ITS poteka skozi razvoj medobratovalnih storitev, s katerimi želimo v prometnem sistemu doseči določen učinek. Razvoj storitev na nivoju celotne platforme C-Roads zagotavlja medobratovalnost in harmonizacijo posamičnih lokalnih implementacij na nivoju celotne platforme. Zaradi večje sprejemljivosti za uporabnike C-Roads predvideva, da se uvedba posamičnih storitev izvede na celotnem območju članic. Zato na nivoju platforme obstaja usklajen dogovor glede nivoja razpoložljivih storitev (Day 1, Day 1.5, Day 2). Uvajanje storitev nato poteka na nacionalnem nivoju skozi implementacijo scenarijev (primerov uporabe) v obliki nacionalnih pilotnih projektov. Pilotni projekti morajo upoštevati skupne dogovore in specifikacije, npr. specifikacije komunikacijskih protokolov ter specifikacije za zagotavljanje varnosti in zasebnosti. Preizkušene lokalne pilotne rešitve je potrebno testirati v čezmejnem okolju, da se zagotovi mednarodna interoperabilnost. Slika 1 (levo) prikazuje organizacijsko shemo kroga sprejemanja odločitev o storitvah ter izvedbe skozi pilotne projekte, Slika 1 (desno) pa prikazuje potek implementacije storitve od vizije zelenih učinkov, skozi oblikovanje scenarijev in vse do operativne faze določene storitve. Ena storitev lahko vsebuje več scenarijev, posamični scenarij pa je lahko apliciran tudi v različnih storitvah. Npr. scenarij »zaprt vozni pas« se lahko uporabi tako v storitvi »delo na cesti« kot v storitvi »obvestilo o nevarni lokaciji«.



Slika 1 - Platforma C-Roads in proces uvajanja storitev ¹

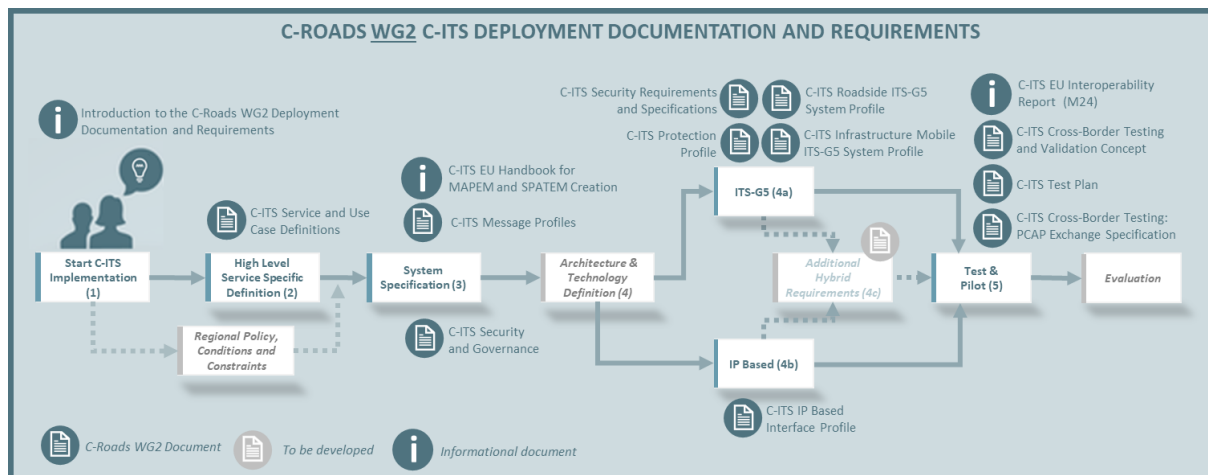
Organizacijsko je platforma C-Roads zastavljena kot konzorcij lastnikov in upravljalcev infrastrukture v sodelovanju z zasebnimi partnerji in organizacijami. V Sloveniji je vlogo nacionalnega partnerja prevzel DARS, ki je od vzpostavitve platforme do sedaj izvajal pilotne projekte uvajanja storitev in scenarijev ter skrbel za njihovo čezmejno testiranje. Iz vidika slovenskega sistema C-ITS DARS prevzema vlogo ponudnika storitev C-ITS, operaterja infrastrukture ter operaterja C-ITS storitev, ki storitve tudi zagotavlja končnim uporabnikom. Projekt, ki je predmet te specifikacije, predvideva vključitev implementacije DARS v nacionalni sistem, ki bo integriran skozi Nacionalno centralno vozlišče C-ITS (angl. National central C-ITS node), kot je opisano v poglavju Vsebina naročila. Le-to bo vzpostavljeno na Nacionalni točki dostopa (NAP) in bo omogočalo vključevanje novih deležnikov, ki bi v prihodnje želeli ponujati svoje storitve v sistemu C-ITS. V tem širšem kontekstu je potrebno upoštevati, da implementacija nacionalnega vozišča mora upoštevati vse specifikacije platforme C-Roads.

Platforma C-Roads predvideva širok nabor postopkov za preverjanje storitev in scenarijev glede sprejemljivosti za uporabnike, glede ustreznosti funkcionalnosti, glede na družbeno ekonomske učinke, prometno varnost, učinkovitost prometa in okoljske vplive. V ta namen infrastruktura C-ITS zbira številne podatke o vedenju udeležencev v prometu, med drugim hitrost, pospeške, menjavo voznega pasu. Nekateri od podatkov, ki jih zbira C-ITS, so občutljive narave, zato je nujno upoštevati specifikacije C-Roads glede zaščite podatkov.

Ob omenjenih varnostnih specifikacijah je osnova harmonizacije in zagotavljanja medobratovnosti celotnega sistema in storitev C-ITS nabor usklajenih in sprejetih specifikacij C-Roads, ki skupaj tvorijo harmoniziran komunikacijski profil (ang. harmonised communication profile). Platforma C-Roads zagotavlja, da je nabor specifikacij vsakih šest mesecev posodobljen z zadnjo verzijo standardov, specifikacij, varnostnih vprašanj, potrjenih storitev ter scenarijev, profilov sporočil C-ITS in parametrov, profilov ITS-G5 in mobilnih (na IP osnovanih) komunikacij ter informacij za čezmejno testiranje storitev. Slika 2 prikazuje strukturo ter sosledje dokumentov, ki jim je potrebno slediti pri razvoju in uvedbi storitev C-ITS. Celoten harmoniziran komunikacijski profil je prosto dostopen na spletni strani C-Roads (www.c-roads.eu) in predstavlja tako organizacijski kot tehnični temelj usklajevanja C-ITS v Evropi.

¹ Vir: The C-Roads Platform, An overview of harmonised C-ITS deployment in Europe
Ecosystem for fully operational C-ITS - The infrastructure perspective
WG1 – C-ITS Organisation (www.c-roads.eu) ; V 0.91, 03.2022

Storitve C-ITS za svoje delovanje potrebujejo komunikacijske tehnologije. C-Roads predvideva, da se za komunikacijo uporabljajo tehnologije ETSI ITS-G5 ali obstoječa mobilna omrežja. Platforma C-Roads predvideva tudi hibridno uporabo obeh navedenih komunikacijskih tehnologij. Sledenje specifikacijam za oblikovanje sporočil določajo tako strukturo, vsebino kot tudi poimenovanja sporočil. Ustrezno oblikovana sporočila, ki se prenašajo skozi omenjena omrežja, omogočajo, da vozila v vseh državah in regijah lahko na enak način komunicirajo s prometno infrastrukturo in drugimi vozili. V vseh treh primerih je nujno zagotoviti varno izmenjavo podatkov skladno z infrastrukturo javnih ključev (angl. Public Key Infrastructure – PKI).



Slika 2. Struktura dokumentov informacijskega profila C-Roads²

Kot je razvidno iz slike, podrobnejše tehnične specifikacije opredeljujejo naslednji dokumenti:

- opis dogovorjenih storitev in scenarijev: C-ITS Service and Use Case Definitions,
- sistemske specifikacije, ki se uporabijo neodvisno od izbire tehnoloških rešitev za komunikacijo ali arhitekturo zalednega sistema:
 - o opis sporočil: C-ITS Message Profiles
 - o varnostne specifikacije: C-ITS Security & Governance
 - o priporočila za opis topologije cest in križišč in zapisa za upravljanje signalov semaforjev: European Handbook for MAPEM/SPATEM creation
- specifikacija za izmenjavo poročil v omrežju 5G:
 - o C-ITS Roadside ITS G5 Profile
 - o C-ITS Infrastructure Mobile ITS G5 System Profile
 - o C-ITS Protection profile
- specifikacija za izmenjavo sporočil IP: C-ITS IP Based Interface Profile
- varnostne specifikacije za C-ITS 5G in IP: C-ITS Security Requirements & Specifications
- specifikacije za preverjanje zagotavljanja čezmejne interoperabilnosti:
 - o C-ITS Cross-Border Testing and Validation Concept
 - o C-ITS Test Plan
 - o C-ITS Cross-Border Testing: PCAP Exchange Specification
 - o C-ITS EU Interoperability Report

Platforma C-Roads ne predpisuje arhitekture in tehnologije za izvedbo nacionalnega sistema C-ITS. V Sloveniji je predvidena izvedba Nacionalnega centralnega C-ITS vozlišča («National central C-ITS node»), ki je glavni predmet pričujoče naloge. Le-ta mora vsebovati Centralno postajo C-ITS, ki

² Vir: Introduction to the C-Roads WG2 Deployment Documentation and Requirements
V 2.0.5, C-Roads Platform, WG 2 Technical Aspects (www.c-roads.eu),

sprejema informacije in oblikuje sporočila skladna s specifikacijami C-ROADS ter izmenjevalno vozlišče, ki omogoča čezmejno izmenjavo podatkov z drugimi nacionalnimi/regionalnimi sistemi (sistem implementira »Improved Interface«). Centralno vozlišče posreduje sporočila ponudnikov v infrastrukturo C-ITS, ki komunicira z uporabniki in je izvedena skladno z zahtevami podanimi v zgoraj navedenih specifikacijah (sistem implementira C-ROADS Basic Interface). Pri izvedbi centralnega vozlišča je nujno zagotoviti skladnost posredovanih sporočil vsem elementom infrastrukture na način, da ohranjajo skladnost s specifikacijami na vseh nivojih izmenjave informacij. Izmenjevalno vozlišče mora zagotavljati izmenjavo informacij s tujimi sistemi skladno s specifikacijami, kar je potrebno preveriti na način, kot predvidevajo zgoraj navedene specifikacije za čezmejno testiranje sistema in zagotavljanje čezmejne interoperabilnosti.

2.2 Piloti DARSa

V okviru platforme C-Roads se uvajanje C-ITS najprej predvideva na avtocestah, ker so tam hitrosti višje, hkrati je manj nepredvidenih dejavnikov, ki bi vplivali na promet, so pa posledice neželenih potekov navadno hujše.

V letih 2016-2020 je v okviru projekta »C-Roads Slovenija« začela vzpostavitev pilotne hibridne rešitve C-ITS 5G in 3G/4G/LTE na primorskem kraku avtoceste A1, na 30 kilometrskem odseku med Postojno in Divačo. Do leta 2020 je bilo na avtocestnem omrežju vzpostavljenih 9 stacionarnih in ena mobilna ITS-G5 obcestna enota (angl. roadside units – RSO).

Pilotni projekti nadgrajujejo in integrirajo obstoječe rešitve ITS in digitalno infrastrukturo slovenskih avtocest, ki avtomatizirano zajema podatke o prometu s pomočjo kamer, števecv prometa, vremenskih postaj in drugih senzorjev. Kot osnova so uporabljeni obstoječi sistemi za posredovanje signalizacije in drugih obvestil voznikom. DARS razpolaga s sistemom za nadzor in upravljanje prometa v predorih ter sistemom za nadzor in upravljanje prometa na tveganih avtocestnih odsekih. Oba sistema sta povezana in delujeta usklajeno. Tretji sistem, to je sistem za prometne informacije, sprejema informacije iz obeh navedenih sistemov in jih posreduje uporabnikom avtocest preko sistema spremenljive prometne signalizacije s pripadajočimi senzorji in sistema za obveščanje uporabnikov.

V okviru platforme C-Roads je DARS skozi pilotne projekte implementiral in vpeljal storitve C-ITS:

- »Opozorilo o delih na cesti« (angl. Road Works Warning – RWW),
- »opozorilo o nevarnih lokacijah« (angl. Hazardous Locations Notification – HLN) ter
- »prenos prometne signalizacije v vozilo« (angl. In-Vehicle Signage – IVS).

Storitev RWW zajema več scenarijev, in sicer zapora enega ali več voznih pasov (RWW-LC), obveščanje o predvidenih zaporah ceste (RWW-RC), premične zapore ceste (RWW-RM) ter zimsko vzdrževanje (RWW-WM).

Storitev HLN zajema večje število scenarijev, kot so prometna nesreča (HLN-AZ), vožnja v nasprotni smeri (HLN-AWWD), prometni zastoj (HLN-TJA), stoječe vozilo (HLN-SV), slabi vremenski pogoji (HLN-WCW), spolzko cestišče (HLN-TSR), oseba ali žival na cestišču (HLN-APR), ovira na cestišču (HLN-OR), nezavarovana zapora ceste (HLN-UBR). Med scenarije obveščanja o nevarnih lokacijah prištevamo tudi obveščanje o vozilih na nujni vožnji, tako reševalcev (HLN-ERVI), kot drugih vozil s prioriteto (HLN-EPVA). HLN zajema tudi nekatere scenarije, ki za avtocestno omrežje niso aktualni, kot npr. križišče z železniško progo (HLN-RLX), križanje z vozilom javnega prometa (HLN-PTVC) ali stoječe vozilo javnega prometa (HLN-PTVS).

Storitev IVS zajema scenarije, ki omogočajo vidnost prometne signalizacije v samem vozilu in ne le na napravah cestne infrastrukture, kar je koristno predvsem v pogojih slabe vidljivosti ter v času spremenljivih sporočil. Scenariji zajemajo informacije o prometnih znakih (IVS-TS) ali drugih besedilnih obvestilih (IVS-FT), namenjeni pa so prikazu informacij o dinamičnih omejitvah hitrosti, navodilom o uporabi določenih voznih pasov, nasvetom glede prehitevanja, drugim znakovnim informacijam ter prikazu besedil portalov VMS.

Celotna infrastruktura je nadgrajena tako, da podpira kodirano komunikacijo z uporabo digitalnih certifikatov in PKI. Za komunikacijo z vozili in obveščanje DARS sistem podpira tako tehnologijo G5, kot obstoječe mobilno omrežje 3g/4g/LTE.

Kot osrednji sistem in orodje za obveščanje DARS uporablja informacijski sistem Kažipot, ki informacije po številnih informacijskih kanalih posreduje v druge sisteme, npr. na portal www.promet.si, mobilno aplikacijo Promet+, teletekst RTV Slovenija, na telefonski odzivnik, prav tako pa obvešča Operativno komunikacijske centre in Policijo ter medije. Z nadgradnjo oziroma povezavo sistema Kažipot s C-ITS je sedaj lokacijsko in časovno aktualna sporočila mogoče posredovati tudi neposredno v vozila. Prav tako pa sistem C-ITS lahko neposredno v sistem Kažipot posreduje aktualne informacije, ki jih sporočajo vozila o stanju v prometu preko postaj RSU. Za potrebe dinamične signalizacije in storitev prenosa prometne signalizacije v vozila (IVS) DARS načrtuje še integracijo vzdrževalnih in drugih vozil DARS (s premično signalizacijo), ki lahko preko sistema C-ITS prejemajo informacije o dinamični signalizaciji, prav tako pa v sistem posredujejo aktualne prometne informacije.

Nadalje se v okviru projekta C-Roads Slovenija 2 (2018-2023) vzpostavlja širitev obcestne infrastrukture C-ITS, ki bo pokrila celotno avtocesto A1, vključno z vmesnikom DARS C-ITS IP in centralnim strežnikom za avtocestno omrežje.

3 Vsebina naročila

Kooperativni inteligentni transportni sistemi uporabljajo tehnologije, ki omogočajo komunikacijo med vozili, komunikacijo s prometno signalizacijo in obcestno infrastrukturo, oziroma z drugimi udeleženci v prometu. Sistemi so poznani tudi z nazivi komunikacija vozilo-z-vozilom (V2V, angl. vehicle-to-vehicle), komunikacija vozilo-z-infrastrukturo (V2I, angl. vehicle-to-infrastructure) ter komunikacija infrastruktura-z-vozilom (I2V, angl. infrastructure-to-vehicle).

V Sloveniji v zadnjih letih že potekajo aktivnosti na področju vzpostavitve sistemov C-ITS v okviru projekta C-Roads pri čemer je bilo zaključenih nekaj pilotnih projektov, ki z obcestnimi enotami C-ITS G5 enotami (RSU, angl. road side units) pokrivajo krajši odsek AC in nekaj predorov.

Hkrati sta bili na področju C-ITS uspešno preizkušeni dve komunikacijski tehnologiji G5 (mikrovalovna) in mobilna (3g, 4g, LTE) z internim in čezmejnim testiranjem.

Slovenija je pri snovanju sistema C-ITS vključena v mednarodni projekt C-Roads. V okviru tega projekta se oblikujejo skupni pristopi, protokoli in specifikacije. Ekspertne skupine intenzivno delajo pri oblikovanju arhitekture storitev, ki ne bi bile vezane le na eno komunikacijsko tehnologijo oz. bi bile v tem smislu nevtralne. Temu razvoju morajo slediti vsi projekti v Sloveniji na tem področju, tudi pričujoči, ki postavlja nacionalni okvir delovanja C-ITS in zagotavlja pogoje za skupen in usklajen razvoj. V tem oziru je projekt nadgradnja in razširitev pilotnih projektov C-Roads Slovenija v okviru platforme C-Roads in pripadajočih delovnih skupin, v okviru katerih se razvijajo kooperativni sistemi C-ITS. Pri izvedbi je nujno zagotoviti skladnost z vsemi specifikacijami C-Roads ter preizkusiti interoperabilnost z obstoječimi sistemi drugih držav, skladnimi s specifikacijami C-Roads, in to na način, kot je opredeljeno v testnih scenarijih projekta C-Roads.

V okviru naloge mora izvajalec preučiti zadnje specifikacije na tem področju, ki so dostopne preko projekta C-Roads in spremljati razvoj. V prvi fazi mora izdelati sistem v skladu s specifikacijami, ki bodo veljavne ob podpisu pogodbe. Ker gre za kontinuiran razvoj, ki ga želi naročnik spremljati tudi na področju t.i. implementacije in ne zgolj na področju specifikacij, je predvidena določena količina ur za nadgradnje in razvoj sistema. Ob koncu projekta mora biti celoten sistem izveden v skladu s takrat veljavnimi specifikacijami.

3.1 Namen in cilji

V okviru naročila se bo izvedla vzpostavitev strežniške infrastrukture, ki zagotavlja:

- Vzpostavitev Nacionalnega centralnega vozlišča C-ITS (angl. National central C-ITS node) s tremi podsistemi:
 - Centralna postaja C-ITS (angl. Central C-ITS station)
 - Platforma za izmenjavo standardiziranih sporočil C-ITS z zunanjimi deležniki vključno s čezmejno izmenjavo (angl. Interchange entity)
 - Nabor vmesnikov (angl. Middleware/C-ITS broker) za izmenjavo podatkov z obstoječimi in bodočimi akterji C-ITS, ki zagotavljajo podatke za delovanje predvidenih storitev sistemov C-ITS.

Z omenjeno strežniško infrastrukturo bo možno povezati vsa sporočila C-ITS pod enotno nacionalno okrilje. Celoten sistem bo omogočal integracijo podatkovnih virov za potrebe storitev C-ITS, prav tako pa se bodo na ta način v nacionalno centralno vozlišče C-ITS lahko povezale obstoječe in bodoče obcestne postaje C-ITS iz državnega in drugih (npr. občinskih) cestnih omrežij, ki zagotavljajo komunikacijo z vozili. Pri izvedbi je potrebno zagotoviti hibridno delovanje sistema, kar pomeni zagotavljanje komunikacij med vozili in infrastrukturo tako z uporabo mikrovalovne tehnologije C-ITS G5, kakor tudi komunikacije C-ITS z uporabo mobilnih tehnologij 4G/5G. Podrobneje je zgradba pričakovanega sistema opredeljena v poglavju Shema sistema.

Predmet tega naročila je tudi implementacija določenih storitev in scenarijev C-ITS. Nacionalno centralno vozlišče C-ITS mora na osnovi podatkov pridobljenih od drugih ponudnikov ali iz informacijskih sistemov NCUP ter iz s tehnologijo C-ITS opremljenih vozil ustvarjati vsebinsko ustrezna sporočila C-

ITS v formatih in ustreznih sosledjih, kot to predvidevajo specifikacije predvidenih scenarijev. Podrobneje je nabor zahtevanih storitev in scenarijev opredeljen v poglavju Storitve in scenariji.

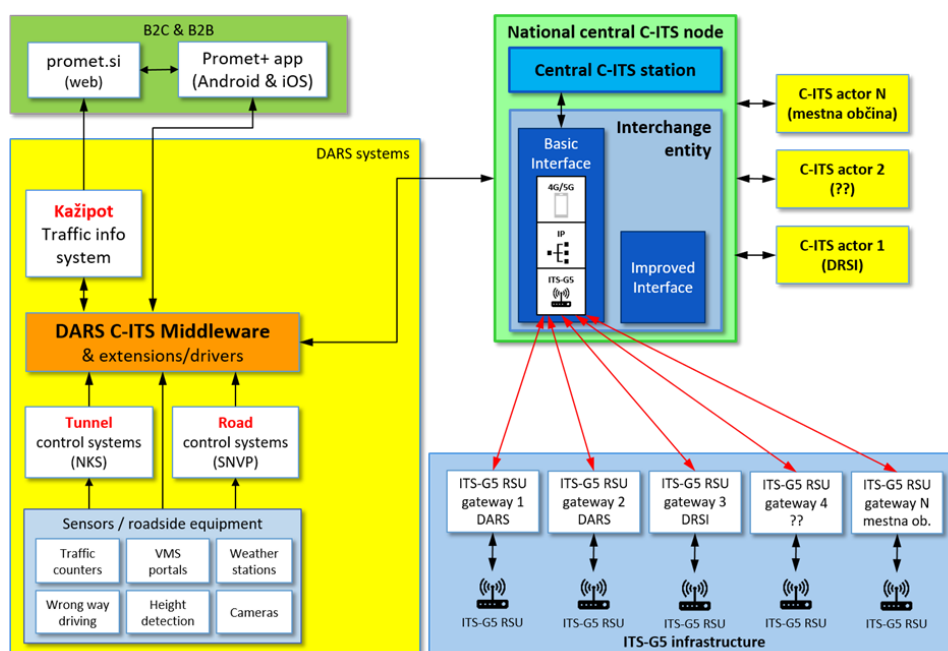
Zagotavljanje storitev C-ITS v oblaku in komunikacije v hibridni kombinaciji komunikacijskih tehnologij, oboje v realnem času, morajo zagotavljati pokrivanje 600 km avtocestnega omrežja, kakor tudi 6000 km sekundarnega omrežja državnih cest.

Izvajalec mora izvedeni sistem integrirati v informacijsko okolje NCUP in ga povezati z vsemi potrebnimi drugimi orodji.

3.2 Shema sistema

V nadaljevanju je v dveh shemah prikazan princip organizacije sistema C-ITS, ki omogoča povezovanje različnih obstoječih in bodočih ponudnikov informacij.

Prva shema (Slika 3) prikazuje pričakovano strukturo C-ITS, ki jo gradi Slovenija. Okvir v svetlozeleni barvi prikazuje t.i. nacionalno centralno vozlišče C-ITS (angl. National central C-ITS node), ki je osrednji cilj naročila. Na ta del se lahko povezujejo različni ponudniki (okvirji v rumeni barvi). Med njimi je trenutno aktiven DARS s svojimi sistemi.



Slika 3. Shema C-ITS sistema v Sloveniji

Vsi nazivi, ki se v shemi uporabljajo za poimenovanje komponent sistema C-ITS so povzeti in skladni z definicijami projekta C-Roads in jih je na ta način potrebno tudi razumeti (glej informacijski profil C-Roads³). Nazivi komponent sistema DARS so povzeti po specifikacijah DARS.

Nacionalno centralno vozlišče C-ITS zajema centralno postajo C-ITS (angl. Central C-ITS Station) ter izmenjevalno vozlišče, v skladu s specifikacijami C-Roads (WG2/TF4 – delovna skupina 2, podskupina 4 za hibridno komunikacijo). Centralna postaja C-ITS oblikuje vsebino sporočil C-ITS za potrebe storitev in scenarijev C-ITS. Sporočila posreduje izmenjevalnemu vozlišču, kjer deluje t.i. Basic Interface (BI), ki opremi vsebino sporočila z meta podatki, potrebnimi za filtriranje in izmenjavo sporočil med akterji in vozlišči sistema skladno s standardi ETSI⁴ ter posreduje sporočila v omrežje. Sestavni del

³ Harmonised C-ITS specifications for Europe (<https://www.c-roads.eu/platform/get-in-touch.html>)

⁴ seznam referenčnih standardov ETSI, C-ITS Message Profiles, C-RRoads Platform, WG2, V 2.0.5, str. 98

izmenjevalnega vozlišča mora biti tudi t.i. Improved Interface (II), ki je namenjen nadzoru pretoka informacij med akterji, še posebej v mednarodnem prostoru. Preko II se akterji med seboj na zaupanja vreden način sporazumevajo glede registracije in kofiguracije naročanja na informacijske vsebine in si izmenjujejo informacije o razpoložljivih vsebinah in zmožnostih sistema.

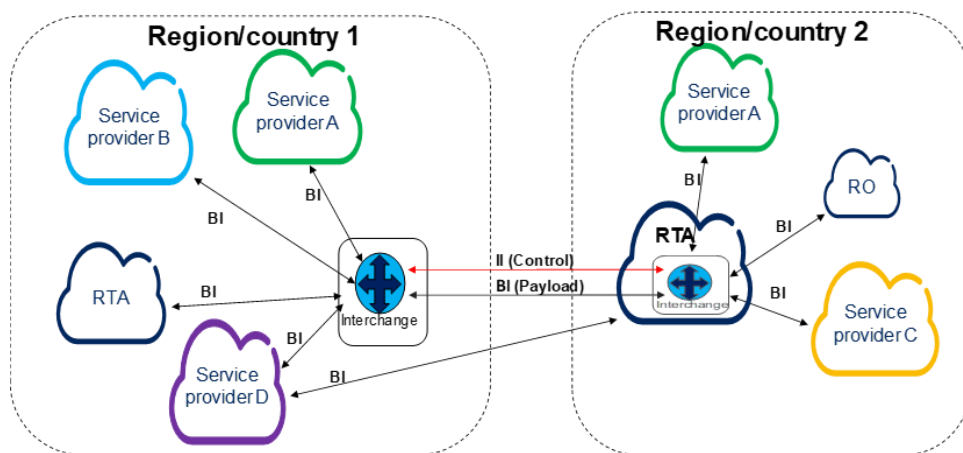
Podatki v centralno vozlišče C-ITS prihajajo od različnih ponudnikov, ki so na sliki prikazani kot okvirji rumene barve. Sodelujoče ponudnike imenujemo tudi akterji C-ITS (angl. C-ITS actor). V bodoče se pričakuje, da bo vse več informacijskih ponudnikov priključenih v sistem in bodo zagotavljali podatke za različne storitve in scenarije C-ITS. Akter C-ITS lahko v centralno vozlišče podatke posreduje v standardizirani obliki kot BI skladno sporočilo, kot je to v primeru sistema DARS, ki sporočila BI generira z vmesno programsko opremo DARS C-ITS, ali pa kot sporočilo »ne-BI« (npr. DATEX, zasebni formati...). Sistem, ki je predmet tega naročila, mora zagotoviti, da v primeru sporočil skladnih z BI centralno C-ITS vozlišče le-ta neposredno posreduje preko izmenjevalnega vozlišča v cestno infrastrukturo C-ITS, mobilna omrežja IP ter z uporabo protokola IP drugim izmenjevalnim vozliščem, ki so naročeni na informacije. V tem primeru centralna postaja C-ITS deluje kot posrednik oz. broker (angl. C-ITS broker). V primeru vhodnega toka »ne-BI« pa centralna postaja C-ITS najprej vsebino pripravi v obliki standardiziranih sporočil BI glede na specifikacije in zahteve podane v opisu storitev C-ITS in scenarijev, nato pa jih posreduje naprej enako kot prej omenjena sporočila BI.

Sporočila C-ITS se distribuirajo po infrastrukturi C-ITS (na sliki moder okvir ITS-G5 infrastructure) do vozil, prav tako pa vozila lahko zagotavljajo informacije o stanju v prometnem toku, ki se posredujejo v centralno vozlišče C-ITS. Prejeta sporočila centralna postaja C-ITS uporabi kot vhod za izvedbo storitev in scenarijev, ki jih sistem podpira. Prometne informacije prejete od vozil je potrebno v nepodvojeni in prečiščeni obliki posredovati tudi v prometnoinformacijski sistem (PIS). Od vozil vedno prihajajo sporočila skladna z BI. Uporaba sporočil BI, ki se posredujejo v vozila, vozilom zagotavlja, da sistemi v vozilih znajo dekodirati in pravilno interpretirati prejeta sporočila za potrebe prikaza na različnih napravah v vozilu (npr. navigacijski in drugi sistemi sporočanja v vozilih). Na shemi ni razvidno, vendar mora BI centralnega vozlišča C-ITS sporočila BI vozilom posredovati tudi z uporabo tehnologije IP mobilnih omrežij 4G/LTE/5G, kar bo zagotovilo hibridno delovanje sistema (mobilno IP 4G/LTE/5G in mikrovalovno G5).

Za potrebe delovanja sistema C-ITS, ki zajema tako distribucijo sporočil C-ITS kakor tudi sprejemanje sporočil iz vozil, je predmet tega naročila vzpostavitev komunikacije IP nacionalnega centralnega vozlišča C-ITS z drugimi sistemi. Med te prištevamo komunikacijo z izmenjevalnimi vozlišči drugih sistemov, npr. tujimi nacionalnimi ali regionalnimi sistemi in vozlišči, ki so naročeni na sporočila slovenskega nacionalnega vozlišča C-ITS. Poleg tega je treba zagotoviti komunikacijo IP preko mobilnih omrežij 4G/LTE/5G z vozili opremljenimi z namenskimi napravami OBU ter komunikacijo IP s strežniki, ki krmilijo gručo postaj C-ITS G5 (RSU).

Komunikacijo s tujimi vozlišči prikazuje naslednja shema (Slika 4). Slika prikazuje strukturo C-ITS, ki je usklajena na ravni projekta C-Roads in omogoča mednarodno povezovanje, kar je nujno za neoviran pretok informacij pri vožnji prek meja različnih držav.

Na shemi prikazan okvirček z nazivom Interchange predstavlja nacionalno centralno vozlišče C-ITS, ki vsebuje izmenjevalno vozlišče (angl. Interchange entity), kot ga prikazuje Slika 3. Izmenjevalna vozlišča se med seboj povezujejo preko BI in II. Vozlišča vmesnik II uporabljajo za registracijo in naročanje na informacijski tok BI, sporočila BI pa zagotavljajo prenos informacijskih vsebin za potrebe storitev C-ITS in scenarijev v sosednjih nacionalnih ali regijskih sistemih C-ITS. V splošnem je lahko nacionalni ali regijski sistem C-ITS zasnovan centralizirano ali distribuirano. V Sloveniji težimo k centralizirani arhitekturi, kot je prikazano v shemi (npr. okvir Country 1), čeprav določeni akterji C-ITS oziroma ponudniki storitev, za potrebe določenih scenarijev med seboj neposredno izmenjujejo informacije na medsebojno dogovorjen način, ki je drugačen od BI. Primer tega je prikaz cestnih zapor na državnih cestah, kjer DRSI te informacije posreduje DARS, le-ta pa poskrbi za generiranje ustreznih sporočil C-ITS, ki jih nato preko nacionalnega centralnega vozlišča C-ITS distribuira v omrežje C-ITS.



Slika 4. Arhitektura za izmenjavo informacij med državama⁵

Z vidika zagotavljanja podatkov za izmenjevalno vozlišče bosta primarna ponudnika DRSI za omrežje državnih cest in DARS za avtocestno omrežje, v prihodnosti pa se pričakuje, da se bodo kot ponudnik podatkov pojavila tudi večja mesta (Ljubljana, Maribor, ...) in različne intervencijske službe, tako da mora biti rešitev narejena tako, da bo možno vključevati nove ponudnike vsebin C-ITS.

K zgoraj opisanemu je dodatno pri implementaciji potrebno upoštevati standarde in smernice razvite v okviru projekta C-Roads, s posebnim poudarkom na rezultatih skupine TF4, ki se ukvarja s hibridno oziroma IP komunikacijo, ter zagotoviti skladnost z zadnjo aktualno verzijo informacijskega profila C-Roads³, pri čemer je potrebno upoštevati, da skupina TF4 še vedno posodablja specifikacije in pripravlja nove verzije. Na nacionalnem nivoju je potrebno izmenjevalno vozlišče oz. entiteto (angl. Interchange Entity), ki bo preko BI (angl. Basic Interface) združevalo podatke različnih ponudnikov podatkov C-ITS vzpostaviti v okviru Nacionalne točke dostopa (NAP, www.nap.si). Vozlišče mora biti izdelano v skladu s specifikacijami skupine WG2, podskupine TF4 projekta C-Roads, pri čemer mora poleg BI podpirati tudi II ter predpisane protokole za varno komunikacijo, da bo lahko vključeno v omrežje zaupanja vrednih evropskih izmenjevalnih vozlišč. Podrobnosti glede zahtev za vmesnike in varnostne protokole so definirane v informacijskem profilu C-Roads in jih izvajalec mora v celoti upoštevati pri implementaciji sistema.

3.3 Storitve in scenariji

Iz funkcionalnega vidika mora nacionalno centralno vozlišče C-ITS kot posrednik podpirati vse z informacijskim profilom C-Roads opredeljene scenarije in sporočila, ki jih lahko zagotavljajo zunanji akterji C-ITS ali jih zagotavlja centralno vozlišče C-ITS samostojno. Na osnovi razpoložljivih podatkov o dogodkih v cestnem omrežju, ki jih je mogoče prodobiti od drugih akterjev ali iz informacijskega sistema NCUP, izvajalec zagotovi, da bo centralno vozlišče samostojno implementiralo spodaj navedene vsebinske sklope oziroma scenarije, ki se nanašajo na nacionalno cestno omrežje.

Pri vsakem scenariju navedenem v tej specifikaciji je opredeljena referenca na opis scenarija (v obliki kratice scenarija, npr. HLN-TJA) v trenutni verziji dokumenta C-ITS Service and Use Case Definitions⁶. Izvajalec mora pri implementaciji scenarijev slediti zahtevam in specifikacijam opredeljenih v informacijskem profilu C-Roads. Izvajalec mora slediti prihodnjemu razvoju informacijskega profila C-Roads in pri implementaciji upoštevati vse morebitne spremembe, ki bodo nastale v dokumentaciji C-Roads med izvajanjem projekta.

⁵ vir: C-ITS IP Based Interface Profile 2.0.1, C-Roads Platform, WG 2 Technical Aspects (www.c-roads.eu) Evolved architecture for country/region information sharing

⁶ C-ITS Service and Use Case Definitions, C-Roads Platform, WG2, V 2.0.5

3.3.1 Storitev Prenos prometne signalizacije v vozilo (In-Vehicle Signage - IVS)

Namen storitve je informiranje udeležencev v prometu o aktualnih statičnih in dinamičnih prometnih znakih in obvestilih, ki veljajo na določenem delu cestnega omrežja in se prikažejo na napravah in sistemih v vozilu.

V sklopu storitve je potrebno implementirati dva scenarija, in sicer:

- IVS - Traffic Signs (IVS-TS)
- IVS - Free Text (IVS-FT).

3.3.2 Storitev Opozorilo o nevarnih lokacijah (Hazardous Locations Notification - HLN)

Storitev Opozorilo o nevarnih lokacijah (Hazardous Locations Notification – HLN) je namenjena sporočanju in opozarjanju prihajajočih vozil, ki se bližajo enemu ali več nevarnim dogodkom na cesti. Vozila prejmejo opozorila o vrsti in lokaciji nevarnosti ter trajanju dogodka, če je ta informacija na voljo.

V sklopu storitve je potrebno implementirati naslednje scenarije:

- Traffic Jam Ahead, (HLN – TJA)
- Stationary Vehicle, (HLN –SV)
- Weather Condition Warning, (HLN – WCW)
- Emergency or Rescue/Recovery Vehicle in Intervention (HLN-ERVI)
- Emergency or Prioritized Vehicle Approaching (HLN-EPVA)
- Railway Level Crossing, (HLN-RLX)
- Public Transport Vehicle at a Stop (HLN-PTVS)

3.3.2.1 Informacije o prometnih zastojih in vremenske informacije (HLN-TJA, HLN-SV in HLN-WCW)

Izvajalec podatke o stanju v prometu in vremenske podatke za izvedbo scenarijev HLN-TJA, HLN-SV ter HLN-WCW pridobiva v realnem času iz obstoječih podatkovnih baz, ki so na voljo na NAP.

3.3.2.2 Informacije o vozilih s prioriteto (HLN-ERVI)

Izvajalec mora v sistemu C-ITS v ustreznih standardih zagotoviti informacije o vozilih na nujni vožnji oz. podatke o gibanju intervencijskih vozil, ko imajo vključeno modro luč.

Storitev naj bo izvedena na podlagi podatkov o lokaciji teh vozil (GPS), in sicer za naslednja vozila:

- Reševalna vozila
 - o Vključena morajo biti potencialno vsa vozila reševalnih postaj (javni zavodi in zasebnih koncesionarjev, za katera bodo dostopni podatki o njihovi vsakokratni lokaciji (GPS).
- Vozila gasilcev
 - o Vključena morajo biti vsa vozila gasilcev (poklicnih in prostovoljnih), za katera bo omogočen dostop do podatkov o njihovi vsakokratni lokaciji (GPS).
- Vozila policije
 - o Vključena morajo biti vsa vozila policije, za katera bo omogočen dostop do podatkov o njihovi vsakokratni lokaciji (GPS). Sistem mora biti zasnovan tako, da bo omogočil dodajanje novih podatkov v prihodnosti.

Izvajalec mora predvideti tehnično usklajevanje s posameznimi skrbniki podatkovnih baz. V ta namen naročnik zagotovi sezname, kontaktne osebe in podporo pri organizaciji izvedbe.

Ostale naloge izvajalca:

- Preučiti podatke dobavitelja (gasilci, reševalci, policija) in prilagoditi sistem tako, da bo možen prenos podatkov.
- Zagotoviti standardne vmesnike s tehničnimi specifikacijami, ki so podlaga za ostale ponudnike oz. dolgoročno vzdržnost in povezljivost sistema. Izvajalec določi format pošiljanja podatkov, ki mora podpirati kodiranje vsaj v eni od standardnih oblik, npr. JSON, XML, protobuf, ASN.1).

3.3.2.3 Informacije o stanju na nivojskih železniških prehodih (HLN-RLX)

Izvajalec mora v sistemu C-ITS v ustreznih standardih zagotoviti informacije o stanju na nivojskih železniških prehodih oz. o tem ali je prehod zaprt ali odprt za cestni promet ter čas, v katerem se bo prehod za cestni promet zaprl. Storitev naj bo izvedena na podlagi podatkov Slovenskih železnic (SŽ).

Izvajalec mora predvideti tehnično usklajevanje s skrbnikom podatkovnih baz (SŽ). V ta namen naročnik zagotovi sezname, kontaktne osebe in podporo pri organizaciji izvedbe.

Ostale naloge izvajalca:

- Preučiti podatke dobavitelja (SŽ) in prilagoditi sistem tako, da bo možen prenos podatkov.
- Zagotoviti standardne vmesnike s tehničnimi specifikacijami, ki so podlaga za ostale ponudnike oz. dolgoročno vzdržnost in povezljivost sistema. Izvajalec določi format pošiljanja podatkov, ki mora podpirati kodiranje vsaj v eni od standardnih oblik, npr. JSON, XML, protobuf, ASN.1).

3.3.2.4 Informacije o vozilih javnega potniškega prometa na postajališčih (HLN-PTVS)

Izvajalec mora v sistemu C-ITS v ustreznih standardih zagotoviti informacije o vozilih javnega potniškega prometa, ki so ustavljena na postajališčih, saj predstavljajo potencialno nevarnost zaradi vstopa in izstopa ponikov in vključevanja vozila v promet. Storitev naj bo izvedena na podlagi realno-časovnih podatkov o vozilih javnega potniškega prometa, ki so na razpolago v informacijskem okolju NCUP.

Izvajalec mora predvideti tehnično usklajevanje s skrbnikom podatkovnih baz naročnika. V ta namen naročnik zagotovi kontaktne osebe in podporo pri organizaciji izvedbe.

Ostale naloge izvajalca:

- Preučiti podatke o stanju vozil javnega potniškega prometa v realnem času in prilagoditi sistem tako, da bo možen prenos podatkov.
- Zagotoviti standardne vmesnike s tehničnimi specifikacijami, ki so podlaga za ostale ponudnike oz. dolgoročno vzdržnost in povezljivost sistema. Izvajalec določi format pošiljanja podatkov, ki mora podpirati kodiranje vsaj v eni od standardnih oblik, npr. JSON, XML, protobuf, ASN.1).

3.3.3 Storitev Opozorilo o delih na cesti (Road Works Warning - RWW)

Storitev uporabnikom cest zagotavlja informacije o delu na cestah. Delo na cesti se lahko izvaja na statični lokaciji ali se lokacija dinamično spreminja, prav tako je lahko delo kratkotrajno ali dolgotrajno. Storitev se nanaša na vse posege, ki jih vzdrževalec ceste izvaja, vključno z uporabo vozil vzdrževalca cest.

V sklopu storitve je potrebno implementirati naslednje scenarije:

- Lane closure (and other restrictions) (RWW – LC)
- Road Closure (RWW – PC)
- Road Works – Mobile (RWW-RM)
- Winter Maintenance (RWW-WM)

Storitev naj bo izvedena na podlagi podatkov nacionalne evidence zapor, ki je v nastajanju. Zato se izvajalec glede vira podatkov uskladi z naročnikom. Povezava z nacionalno evidenco zapor je sestavni del integracije predmeta tega naročila v informacijski sistem NCUP.

3.3.3.1 Zimsko vzdrževanje cestišča (Winter maintenance - RWW-WM)

Izvajalec mora v sistemu C-ITS v ustreznih standardih zagotoviti informacije o vozilih, ki jih vzdrževalci cest uporabljajo za izvajanje zimske službe, in sicer med izvajanjem opravil zimskega vzdrževanja cestišča.

Storitev naj bo izvedena na podlagi podatkov o lokaciji teh vozil (GPS). Vključena morajo biti potencialno vsa vozila zimske službe za katera bodo dostopni podatki o njihovi vsakokratni lokaciji (GPS).

Ostale naloge izvajalca:

- Preučiti podatke dobaviteljev (koncesionarji...) in prilagoditi sistem tako, da bo možen prenos podatkov.
- Zagotoviti standardne vmesnike s tehničnimi specifikacijami, ki so podlaga za ostale ponudnike oz. dolgoročno vzdržnost in povezljivost sistema. Izvajalec določi format pošiljanja podatkov, ki mora podpirati kodiranje vsaj v eni od standardnih oblik, npr. JSON, XML, protobuf, ASN.1).

3.3.4 Storitev Semaforizirana križišča (Signalized Intersections - SI)

Križišča so kompleksna prometna okolja, kjer obstaja povečano tveganje prometnih nezgod, prav tako pa v križiščih večkrat prihaja do situacij, ki negativno vplivajo na učinkovitost prometnega toka, posledično se vozila velikokrat ustavljajo in pospešujejo, kar vpliva na povečanje škodljivih emisij.

Namen storitve je izboljšati varnost in pretočnost semaforiziranih križišč ter zmanjšanje onesnaženja okolja. Storitve uporabnikom ceste omogoča prejetje informacij o signalih semaforjev ter posredovanje sporočil krmilnikom semaforjev o prihajajočih vozilih (npr. vozila s prioriteto).

V sklopu storitve je potrebno implementirati scenarij:

- Green Light Optimal Speed Advisory (GLOSA)

3.3.4.1 Implementacija sistema GLOSA (Green Light Optimal Speed Advisory – GLOSA)

Izvajalec mora v sistemu C-ITS zagotoviti informacije o intervalih na semaforstvih sistemih, kar omogoča uvedbo sistema svetovanja voznikom o optimalni hitrosti za zeleno luč, ko pripeljejo v križišče.

Storitev naj bo izvedena na podlagi podatkov s semaforjev na državnih cestah, s katerimi razpolaga DRSI. Prav tako morajo biti uporabljeni podatki o semaforjih, ki jih upravljajo posamezne občine, in sicer tisti, ki so v času trajanja projekta na voljo.

Izvajalec mora predvideti tehnično usklajevanje s skrbniki podatkovnih baz (DRSI, občine). V ta namen naročnik zagotovi sezname, kontaktne osebe in podporo pri organizaciji izvedbe.

Ostale naloge izvajalca:

1. Preučiti podatke dobavitelja (DRSI, občine) in prilagoditi sistem tako, da bo možen prenos podatkov.
2. Zagotoviti standardne vmesnike s tehničnimi specifikacijami, ki so podlaga za ostale ponudnike oz. dolgoročno vzdržnost in povezljivost sistema. Izvajalec določi format pošiljanja podatkov, ki mora podpirati kodiranje vsaj v eni od standardnih oblik, npr. JSON, xml, protobuf, ASN.1).

3.3.5 Storitve Podatki o gibanju vozil (Probe Vehicle Data - PVD)

Podatki o gibanju vozila oz. Probe Vehicle Data (PVD) je storitev C-ITS, ki zagotavlja podatke o vozilu drugemu vozilu (t.i. storitev V2V), prav tako pa tudi sistemom upravljavcev cest (t.i. storitve V2I). Cilj storitve je zbiranje podatkov o gibanju vozil, s čimer se izboljša upravljanje prometa in varnost.

V sklopu storitve je potrebno implementirati scenarija:

- Vehicle Data Collection (PVD-VDC)
- Event Data Collection (PVD-EDC)

Storitev zagotavlja podatke za druge storitve C-ITS, ki so predmet tega naročila. Prav tako pa mora izvajalec v sklopu integracije sistema C-ITS v informacijsko okolje NCUP posredovati podatke v druge podatkovne baze NCUP in sisteme (npr. PIS, prometni model in drugi), kar mora izvajalec uskladiti z naročnikom.

3.4 Centralna postaja C-ITS

V sklopu centralnega nacionalnega vozlišča C-ITS je potrebno implementirati centralno postajo C-ITS, ki bo generirala vsebinsko in tehnično pravilna sporočila C-ITS, skladna s standardi ETSI, kot je to

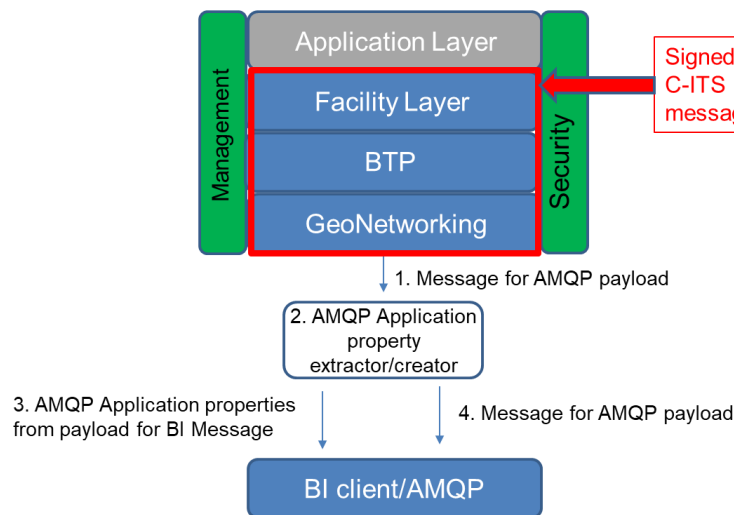
opredeljeno v informacijskem profilu C-Roads. Centralna postaja C-ITS sporočila posreduje na vmesnik BI skladno s predvidenimi scenariji in ta jih distribuira po različnih kanalih (IP, mikrovalovno). Centralna postaja mora tudi pravilno interpretirati vsebino prejetih sporočil C-ITS, ko je to potrebno za potrebe aplikacij, scenarijev in posredovanja podatkov v druge sisteme informacijskega okolja NCUP.

V trenutnem pilotnem sistemu DARS se konkretna sporočila C-ITS ustvarjajo na krmilnikih gruče obcestnih enot (ITS-G5 RSU gateway DARS) na osnovi informacij ustvarjenih v vmesni programski opremi DARS C-ITS (Slika 3) in so posledično na voljo le preko brezžičnega omrežja ITS-G5.

3.4.1 Arhitektura centralne postaje C-ITS

Naslednja shema (Slika 5) prikazuje strukturo centralne postaje C-ITS. Iz sheme je razvidno, da postaja iz podatkovnih virov aplikacij ustvarja vsebino sporočil skladno s specifikacijami BI, ki jih opremi z lupino AMQP za pošiljanje preko omrežja. Sporočila so geo-locirana tako, da jih je mogoče ustrezno geografsko filtrirati pri posredovanju v relevantne dele omrežja. Prav tako so sporočila varnostno podpisana.

Central C-ITS station architecture for Basic Interface



Slika 5. Shema C-ITS postaje za BI (povzeto po specifikaciji C-Roads)

Za potrebe predvidenih scenarijev mora centralna postaja C-ITS podpirati generiranje vseh tipov sporočil predvidenih s Facility Layer Services (FLS) in ki jih zahtevajo specifikacije scenarijev, kot so DENM, IVIM, MAPEM, SPATEM, SREM, SSEM. Za vse podrobnosti za potrebe implementacije, generiranja in interpretacije sporočil izvajalec uporabi specifikacijo C-Roads C-ITS Message Profiles⁷.

Postaja mora omogočati:

- ustvarjanje podpisanih in nepodpisanih sporočil. Pri tem se izvajalec mora držati specifikacij C-Roads navedenih v C-ITS Security Requirements & Specifications⁸ ter C-ITS Security & Governance⁹
- krmiljenje preko vmesnika REST API.

⁷ C-ITS Message Profiles, C-Roads Platform, WG2, TF 3, V 2.0.5

⁸ C-ITS Security Requirements & Specifications, C-Roads platform, WG 2, TF 1, V 2.0.5

⁹ C-ITS Security & Governance, C-Roads platform, WG 2, TF 1, V 2.0.5

- ustvarjanje sporočil C-ITS iz obstoječih standardnih formatov z upoštevanjem navodil za ključna sporočila povezana z varnostjo (TISA SRM) in njihovih pravil za pretvorbo med različnimi standardi:
 - o DATEX II,
 - o TPEG,
 - o RDS-TMC,
 - o drugimi zasebnimi formati skladno z dogovorom z naročnikom.

Postaja mora zagotavljati visoko razpoložljivost in odzivnost.

3.4.2 Geolociranje

Centralna postaja C-ITS, kakor tudi celotno centralno vozlišče mora delovati po principu zavedanja o lokaciji, tako da je možno optimalno obveščanje vozil hkrati pa tudi upravljanje z infrastrukturo. Podatki o lokaciji morajo biti povezljivi s podatkovnim skladiščem ITS, prometnim modelom in platformo FCD, ki za namene C-ITS zagotavljajo podatke o dogodkih, pretočnosti in simulacijah stanja cestnega omrežja (vsi navedeni sistemi so del informacijskega sistema NCUP).

Za lokacijsko referenciranje vhodnih podatkov, ki temeljijo na banki cestnih podatkov (BCP) je potrebno zagotoviti referenciranje na osnovi dinamične segmentacije po BCP ter lokacijski tabeli TMC (DARS 702-35), za vse ostale pa na osnovi dinamičnega referenciranja po metodi OpenLR. Lokacijsko referenciranje izhodnih podatkov mora temeljiti izključno na osnovi lokacijske tabele TMC (DARS 702-35) ter OpenLR¹⁰.

Glede na specifikacijo C-Roads je potrebno zagotoviti preslikavo geo lokacij iz zgoraj navedenih metod referenciranja v »ploščice« po sistemu »quadtree«, zaradi geo-filtriranja sporočil in optimizacije prometa sporočil, kot je predvideno iz specifikacije C-Roads. Podrobnosti o uporabi metode geo-lociranja s »quadtree« so navedene v prilogi Appendix A dokumenta C-ITS IP Based Interface Profile¹¹.

Naloga izvajalca je, da pri implementaciji scenarijev zagotovi ustrezno filtriranje sporočil na osnovi geografske lokacije z namenom optimizacije obsega sporočil v celotnem sistemu C-ITS, še posebej zaradi zagotavljanja zadostne pretočnosti podatkov ter razpoložljivosti in odzivnosti sistema v realnem času. Pri tem mora izvajalec slediti specifikacijam C-Roads glede filtriranja sporočil ter razvijati strategije za optimalno ciljanje sporočil glede na geografsko lokacijo obravnavanega prometnega dogodka. Pri implementaciji mora izvajalec posebno pozornost nameniti prav odzivnosti sistema, pri čemer morajo biti sporočila ponudnikom na voljo prej kot v 30 milisekundah od prispetja v sistem, pri tem pa mora biti sistem sposoben obdelati najmanj 5.000 prejetih sporočil vsako sekundo.

3.4.3 Varnost

Sistem C-ITS lahko prenaša številne informacije o stanju v prometu v vozila ter iz vozil. Podatkovni tok je lahko namenjen informiranju voznika ali pa v bodoče tudi samega vozila, da lahko reagira ustrezno situaciji v prometu. Zato je pomembno, da se voznik ali vozilo lahko zanese na pravilnost, pravočasnost in ustreznost posredovanih informacij. Da bi zagotovili vse navedeno, je v sistemu potrebno zagotoviti informacije iz zanesljivih virov ter na način, ki prejemnikom informacij zagotavlja, da so informacije dejansko prišle iz teh virov. Torej je potrebno zagotoviti varen prenos podatkov med infrastrukturo in vozili. Prav tako pa je potrebno varovati vsebino sporočil. Navedeno velja tako za prenos informacij v kratkem dosegu, torej z mikrovalvono tehnologijo G5, ali na večje razdalje, z uporabo mobilnih tehnologij 4G/5G.

Izvajalec mora pri izgradnji sistema upoštevati smernice projekta C-Roads glede varnega prenosa podatkov in to ne glede na način prenosa. V varnem načinu je sporočila potrebno podpisovati s certifikati, ki omogočajo varno uporabo tudi v čezmejnem prometu.

¹⁰ OpenLR, White Paper v 1.5, http://www.openlr.org/fileadmin/user_upload/openlr-whitepaper_v1.5.pdf

¹¹ C-ITS IP Based Interface Profile, C-Roads platform, WG 2, TF 4, V 2.0.5, str 48.

Glede na to, da specifikacije C-Roads in praksa na področju podpisovanja sporočil in izdajanja certifikatov na nivoju vseh članic EU še ni dokončno dorečena, mora izvajalec v teku projekta spremljati razvoj in prilagajati varno komunikacijo dogovorjenemu načinu med deležniki konzorcija C-Roads, še posebej dokumenta C-ITS Security Requirements & Specifications⁸ ter C-ITS Security & Governance⁹. Trenutno specifikacija predvideva podpisovanje in avtentikacijo vsebine sporočil C-ITS glede na standard ETSI TS 103 097 ter dodatno kodiranje celotnega sporočila s TLS 1.3. Če v teku projekta ne bo mogoče uporabljati korenskih potrdil s strani zaupanja vrednega izdajatelja EU, naj izvajalec preuči možnost vzpostavitve uporabe potrdil nacionalnih zaupanja vrednih izdajateljev.

3.5 Aktivnosti

Na temelju opisa specifikacije predmeta naročila, kot je opisano v predhodnih poglavjih, izvajalec projekt izvede skozi naslednje aktivnosti:

- A1. Izdelava podrobnega terminskega načrta za izvedbo javnega naročila
- A2. Integracija podatkov NAP za potrebe C-ITS
- A3. Izdelava spletnih vmesnikov za zunanje ponudnike informacij
- A4. Izdelava scenarijev C-ITS
- A5. Izdelava vmesnika BI centralne postaje C-ITS
- A6. Izdelava vmesnika II centralne postaje C-ITS
- A7. Integracija podatkov iz C-ITS v NAP
- A8. Testiranje storitev nacionalnega vozlišča C-ITS in centralne postaje C-ITS
- A9. Testiranje II in BI z drugimi nacionalnimi ali regionalnimi sistemi C-ITS
- A10. Dokončni prevzem s poročilom in dokumentacijo ter predano izvorno kodo

Prevzemu rezultatov projekta sledi obdobje pogodbenega vzdrževanja.

4 Nefunkcionalne zahteve

4.1 Uporabnost

Rešitev mora zagotavljati enostavno (intuitivno) uporabo funkcionalnosti. Kjerkoli je to izvedljivo, mora uporabniku ponuditi takojšen odziv (angl. real time response) in biti čim bolj prilagojen učinkoviti uporabi (čim manjše število korakov za izvedbo določenega postopka, čim hitrejši dostop do kakovostnih informacij).

4.2 Razpoložljivost

Razpoložljivost in nekatere ostale karakteristike so zahtevane glede na zahtevano razpoložljivost posameznih funkcionalnosti sistema.

Funkcionalnosti morajo biti razpoložljive 24 ur vse dni v letu. Funkcionalnosti morajo biti razpoložljive 99 % glede na letno raven. Na letnem nivoju je dopustnih največ 87,6 ur izpada.

Pri zagotavljanju zgornje zanesljivosti posamezen izpad ne sme biti daljši od dveh (2) ur.

Vsaka načrtovana prekinitiv delovanja (zaradi npr. nujnih popravkov programske ali strojne opreme, nadgradenj in drugih nujnih del) naročniku sporočena najmanj tri (3) dni pred dejansko prekinitvijo. V sporočilu mora biti naveden razlog za prekinitiv ter čas, v katerem bo izvedena prekinitiv.

Zgornje zahteve se nanašajo na razpoložljivost rešitve in storitev, ki tečejo v okviru rešitve, ne pa tudi na zunanje sisteme, s katerimi se rešitev integrira ali povezuje.

4.3 Zanesljivost

Zaradi zahteve po točnosti podatkov, ki se bodo uporabljali v okviru rešitve, je treba v okviru načrtovanja sistema poseben poudarek nameniti zanesljivosti sistema in njegovih podatkov. V okviru zagotavljanja zanesljivosti je treba zagotoviti več varnostnih in kontrolnih mehanizmov, ki bodo omogočali, da so podatki v sistemu celoviti, točni in odražajo dejansko stanje. Na primer: primerjava vrednosti parametrov uvoženih podatkov z dovoljenimi vrednostmi parametrov (šifranti, tipi, klasifikacije, lokacijske tabele), omejitve in kontrole na nivoju podatkovne baze (constraints).

Visoko zanesljivost je treba zagotoviti tudi na nivoju prenosa podatkov. V okviru prenosa podatkov mora biti zagotovljeno preverjanje celovitosti podatkov (angl. Data Integrity Verification) s funkcijo samodejnega obnavljanja in preprečevanja podvajanja podatkov.

V primeru, da pride do napak ali izpada sistema, mora imeti rešitev zagotovljen mehanizem, ki mu bo omogočal prehod v prvotno stanje.

4.4 Zmogljivost

Rešitev mora biti zasnovana tako, da bo brez težav sposobna:

- zagotavljati nemoteno delovanje in izvajanje funkcionalnosti na produkcijskem okolju s strojno in sistemsko opremo, predvideno ali ponujeno v okviru tega naročila;
- zagotavljati nemoteno izmenjavo podatkov z zunanjimi informacijskimi sistemi, kot je opredeljeno v funkcionalnih zahtevah;
- odzivni čas za prikaz izbranih podatkov na karti ali mapi, ob postavljenih pogojih in kriterijih, ne sme biti daljši od 3s;
- odzivni čas za enostavno poizvedbo in izpis prometnih podatkov na zaslon v obliki tabele (npr. Pregled po dveh dimenzijah in treh parametrih) iz podatkovnega skladišča ne sme presežati 1s,
- odzivni čas uporabniškega vmesnika rešitve za pregled podatkov in prikaz poročil, ki se nanašajo na prostorske podatke, bo natančno opredeljen v okviru aktivnosti analize in specifikacije zahtev končne rešitve. Zahteva naročnika je, da se v okviru aktivnosti analize in specifikacije zahtev opredeli in uskladi tipe vpogleda v podatke in tipe poročil, način njihove

priprave (preko spletnega vmesnika, asinhrona priprava poročil v ozadju, predpriprava poročil itd.) ter zahtevane odzivne čase za posamezno kategorijo. Pri tem mora izvajalec zagotoviti takšne odzivne čase za pripravo vpogledov v podatke in poročila, da bodo omogočali zadovoljivo uporabniško izkušnjo.

V primeru, da izvajalec zahtevanih odzivnih časov ne more doseči, mora identificirati vzrok, ki ga bo obravnaval skupaj z naročnikom. V primeru, da vzrok za performančne težave ne izvira iz drugih sistemov (ki se npr. odzivajo prepočasi pri izmenjavi podatkov itd.), bo moral le-tega odpraviti.

4.5 Nadgradljivost

Rešitev mora biti zasnovana na način, ki bo omogočal enostavno (tehnološko nezahtevno) in hitro izvajanje nadgradenj. Arhitekturna in tehnična zasnova morata omogočati dovolj enostavno dodajanje novih sklopov funkcionalnosti, modulov oziroma rešitev, ki bi izhajale iz naslova novih potreb oziroma zahtev naročnika.

4.6 Skalabilnost

Glede na velik obseg podatkov, ki se bo v prihodnosti še povečeval, mora biti rešitev skalabilna. Povečevanje obsega podatkov ne sme vplivati na poslabšanje zmogljivost sistema.

4.7 Varnost

Komponente rešitve, ki so predmet javnega naročila, morajo biti izdelane z upoštevanjem vseh dobrih praks, ki zagotavljajo zahtevano stopnjo informacijske varnosti.

Izvajalec mora zagotoviti enkripcijo občutljivih podatkov na vseh delih rešitve, kjer prihaja do prenosa podatkov (npr. predvideva se uporabo tehnologij SSL in TLS povsod tam, kjer se prenašajo uporabniška imena in gesla, pomembni sistemski/konfiguracijski podatki, posredujejo osebni podatki ipd.). Občutljivi podatki (osebni podatki, občutljivi osebni podatki, gesla, občutljivi poslovni podatki) morajo biti ustrezno zaščiteni (z enkripcijo) tako med prenosom kot v mirovanju.

Za vsakega uporabnika rešitve bodo določeni nivo in pravice dostopa do podatkov in funkcionalnosti. Vsak uporabnik ima lahko le toliko pravic, kot jih res potrebuje. Rešitev mora zagotoviti naslednje varnostne mehanizme:

- varnostne stopnje;
- za posamezne uporabnike z različnimi pravicami dostopa;
- za skupine uporabnikov z različnimi pravicami dostopa;
- za administratorje;
- pravice do dostopa in nadzor nad dostopi za transakcije (npr. uvoz podatkov ...);
- beleženje vseh dostopov do opredeljenih podatkov v zbirki;
- vzdrževanje gesel;
- avtorizacijo uporabnika;
- zagotavljanje varnosti na mrežnem in sistemskem nivoju, ki jo definira ponudnik na podlagi razpoložljive oz. ponujene opreme in ustreza zahtevam rešitve.

Rešitev mora zagotavljati:

- zagotovljena mora biti nedvoumna identifikacija uporabnika ter beleženje vseh pasivnih in aktivnih dostopov skladno z določbami Zakona o varstvu osebnih podatkov;
- zaradi kasnejšega ugotavljanja morebitnih zlorab je za vsako spremembo pravic za vsakega uporabnika ter za vsak aktivni in pasivni dostop do podatkov visokega razreda varnostnih zahtev s strani uporabnikov treba voditi natančno evidenco -> revizijske sledi;
- revizijske sledi morajo biti po vsebini, hrambi in sistemu nadzora (skupaj z varnostno shemo in povezanimi postopki) ustrezne, tako da zdržijo kot dokazni material pred pravosodnimi organi;
- spletni vmesniki za delo s podatki visokega razreda varnostnih zahtev bodo tekli izključno po dobro zaščitenih vodih s kriptirnim sistemom SSLv3 ali TLS 1.0;

- spletni vmesnik mora biti odporen na penetracijske napade informacijskih sistemov (kot npr. SQL injection, XSS (cross site scripting), file inclusion, error handling, URL parameter manipulation, buffer overflow ...);
- spletni servisi rešitve, ki so dostopni odjemalcem za množično posredovanje ali pridobivanje podatkov, morajo biti zaščiteni pred namernimi napadi s strani zunanjih sistemov, ki bi lahko povzročili nedelovanje storitev (npr. Denial of service attack);
- spletni vmesnik mora imeti vgrajen mehanizem za odjavo uporabnikov v primeru poteka seje – v primeru daljše neaktivnosti rešitve zahteva ponovno prijavo uporabnika;
- rešitev mora biti odporna na vsa tveganja, opredeljena v aktualnem OWASP Top 10 naboru za spletne aplikacije.

Odgovorni in tehnični vodja projekta mora zagotoviti okvirni načrt varnosti za funkcionalno izvajanje rešitve v produkcijskem okolju že ob prvem mejniku M1 ter ga usklajevati z naročnikom in dopolnjevati do zaključka del. Sprotno preverjanje implementacije varnosti s poročilom se izvaja od operativne vzpostavitve naprej. S tem se izvaja razvojni, vzdrževalni in izobraževalni cikel varnostne politike.

Referenca za izdelavo varnostnega načrta so standardi serije ISO 27000. Obseg varnostnega načrta oz. izbor segmentov se uskladi med naročnikom in izvajalcem. Naročnik bo ob zaključku preveril varnostno politiko na osnovi končnega načrta varnosti, po potrebi z neodvisnim zunanjim izvajalcem informacijske varnosti v skladu z ISO 27002 (Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri kontrolah informacijske varnosti / angl. Security Framework Audit Program).

4.8 Tehnološke zahteve

Celotna rešitev mora biti predana in nameščena lokalno pri naročniku.

Za celotno rešitev, razen za sistemsko programsko opremo, mora biti predana izvorna koda ter izdelana in naročniku predana vsa tehnična dokumentacija v tiskani obliki (1 izvod) in v formatih .docx in .pdf v elektronski obliki.

5 Metodološke zahteve

5.1 Vodenje projekta in poročanje na strani izvajalca

Vsak izvajalec posameznega sklopa je tekom izvajanja projekta dolžan na zahtevo naročnika pripravljati plan izvajanja aktivnosti in poročilo o napredku aktivnosti glede na veljavne terminske plane, poročila revizorjem za potrebe pregleda/revizije, ki jih izvaja naročnik, priporočila za morebitne spremembe in dopolnitve zakonodajnega okvira in druga poročila in strokovna mnenja glede na zahteve naročnika.

Tekom izvajanja aktivnosti, ki so predmet javnega naročila, so predvideni koordinacijski sestanki, ki jih bo vodil vodja projekta na strani naročnika z namenom razreševanja odprtih vsebinskih vprašanj in podajanja pojasnil oziroma usmerjanja pri pripravi izdelkov. Vodja projekta posameznega sklopa na strani izvajalca se dolžan redno udeleževati planiranih koordinacijskih sestankov in pripraviti zapis dogovorov sestanka. Na zahtevo naročnika ali izvajalca se po potrebi koordinacijskih sestankov udeležijo tudi ostali člani projektne skupine.

Redno poročanje je mesečno do najkasneje tretji (3) delovni dan v mesecu za pretekli mesec in obsega poročilo v elektronski obliki v verziji, ki jo je mogoče urejati (npr. .doc ali .docx), in v verziji, ki je ni mogoče spreminjati (npr. .pdf)). Poročilo obsega poročilo o opravljenih aktivnostih od začetka projekta s planom aktivnosti do zaključka projekta. Mejniki ter finančna realizacija in plan morata biti podana in razdelana po mesecih. Kolikor naročnik določi predlogo mora biti poročilo izdelano v skladu s predlogo. Izvajalec četrtletno poročilo predstavi na četrtletnem koordinacijskem sestanku katerega izvedba je obvezna za obe strani in za katerega je potrebno izdelati zapis katerega priloga je četrtletno poročilo. Kolikor naročnik zahteva dopolnitev jo je izvajalec dolžan izvesti.

5.2 Metodologija razvoja in terminski načrt

Ponudbi mora izvajalec predložiti predlog podrobnega terminskega načrta. Zahteve za terminski načrt so naslednje:

- terminski načrt mora obsegati aktivnosti, ki so zajete v tehnični specifikaciji in mora biti skladen z zahtevami naročnika iz tehničnih specifikacij. Izvajalec mora pri pripravi terminskega načrta smiselno upoštevati obdobja dopustov, v katerih bodo člani projektne skupine naročnika predvidoma omejeno razpoložljivi v času dopustov;
- predlog terminskega načrta mora vključevati tudi naloge, ki jih bo moral izvesti naročnik ter opis pogojev za izvedbo posameznih aktivnosti, ki jih mora zagotoviti naročnik;
- terminski načrt mora upoštevati časovne roke iz Tehnične specifikacije;
- terminski načrt mora vključevati podrobnejšo razčlenitev aktivnosti glede na podane aktivnosti v tehničnih specifikacijah. Za vsako aktivnost mora biti podan začetek, konec in trajanje;
- predlog terminskega načrta mora naročniku omogočati nadzor nad potekom projekta v časovnem in vsebinskem smislu.

Predlog terminskega načrta bosta naročnik in izvajalec uskladila v okviru zagonskih aktivnosti projekta. Usklajen in potrjen podroben terminski načrt bo podlaga za izvajanje in spremljanje napredka projekta.

Izvajalec mora svoj življenjski cikel razvoja izvajati skladno z zahtevami in splošno sprejetimi standardnimi metodologijami, ki so v svetu široko uporabljane, konkretna metodologija razvoja programske opreme pa ni predpisana.

5.3 Analiza in specifikacija zahtev

Za rešitev mora izvajalec pripraviti podrobno specifikacijo zahtev, s katerimi bodo posledično dosežene višja kakovost, višja učinkovitost in izboljšana koordinacija v razvojnem procesu ter boljši pregled nad napredkom procesa razvoja.

Izvajalec bo zahteve analiziral neposredno s predstavniki ključnih uporabnikov sistema, pri čemer mora uskladiti njihove morebitne med seboj nasprotujoče si zahteve.

Ključni uporabniki, ki bodo sodelovali pri analizi in specifikaciji zahtev, bodo izvajalcu:

- pojasnili vsebino relevantnih poslovnih procesov in specifične izraze;
- sprejemali odločitve v zvezi z zahtevami (ko bo to potrebno);
- pregledali zahteve, prototipe in ostala gradiva;
- čim prej izvajalcu dali informacijo o spremembi zahtev in upoštevali proces spreminjanja le-teh.

Kot podlago za pripravo specifikacije zahtev mora izvajalec preučiti razpisno dokumentacijo in druge dokumente, ki mu jih preda naročnik.

V okviru specifikacije se pričakuje naslednje:

- pripravljena je v slovenskem jeziku;
- uporabljena terminologija bo prilagojena naročniku;
- izvajalec mora spoznati naročnikovo poslovno področje;
- v specifikaciji zahtev uporabljene diagramske in druge tehnike so primerno pojasnjene;
- specifikacija zahtev vključuje zahteve glede uporabnosti rešitve.

Če izvajalec oceni, da drugače ne bo mogel zajeti naročnikovih zahtev za rešitev, mora pri pripravi specifikacije uporabiti prototipe.

Izvajalec mora zajeti:

- funkcionalne zahteve;
- nefunkcionalne zahteve (zmogljivost, varnost ...);
- implementacijske zahteve.

Analizirane zahteve mora izvajalec primerjati z zahtevami, podanimi v tem dokumentu ter ostali predani dokumentaciji, in jih po potrebi uskladiti z naročnikom in uporabniki.

Izvajalec mora podati končen predlog podrobne specifikacije rešitve, jo nato uskladiti z naročnikom ter pridobiti njegovo potrditev specifikacije zahtev.

Naročnikove zahteve po uvajanju sprememb specifikacije so neizogibne, zato jih mora izvajalec ustrezno obvladovati. Skozi ves čas razvoja mora izvajalec specifikacijo zahtev ažurirati in ob njegovem zaključku naročniku predati dokument specifikacije zahtev, ki odraža dejansko stanje razvite rešitve.

5.4 Implementacija rešitve

Na podlagi usklajenega načrta implementacije bo izvajalec izvedel implementacijo skladno s terminskim načrtom. Aktivnosti implementacije bo sledila aktivnosti stabilizacije funkcionalnosti, ki bo potekala vzporedno s testiranjem funkcionalnosti s strani izvajalca. V okviru stabilizacije bo izvajalec odpravljaj napake, ki bodo odkrite v okviru testiranja izvajalca. Na koncu aktivnosti stabilizacije funkcionalnosti mora biti vsa funkcionalnost v skladu s specifikacijo zahtev razvita in ustrezno preverjena s strani izvajalca za predajo naročniku v prevzemno testiranje.

Vzporedno s prevzemnim testiranjem funkcionalnosti bo izvajalec odpravljaj morebitne pomanjkljivosti, ki jih bo ugotovila projektna skupina naročnika in vključene institucije.

5.5 Namestitev rešitve

Izvajalec bo sodeloval pri nameščanju rešitve na testno in produkcijsko okolje pri naročniku. Nameščanje v testno okolje bo izvajal izvajalec ali po odgovoru skrbnik naročnikove infrastrukture, ki ga bo zagotovil naročnik. Nameščanje v produkcijsko okolje bodo v skladu z opredeljenimi pravili izvajal skrbnik naročnikove infrastrukture.

Za vsako namestitev novega modula ali popravka obstoječega modula rešitve mora izvajalec pripraviti ustrezna navodila za namestitev.

Nove verzije/popravki modulov se najprej namestijo na testno okolje pri naročniku. Odgovorni predstavnik izvajalca opravi najmanj naslednja preverjanja:

- da je bila namestitve opravljena v skladu s izvajalčevimi navodili;
- da rešitev deluje v skladu s funkcionalnimi pričakovanji;
- da je rešitev tudi performančno ustrezna in deluje v skladu s pričakovanji.

Šele na podlagi pozitivnega izida tega potrditvenega testa, izjave odgovornega, da je bil test pozitivno opravljen, se lahko rešitev namesti na produkcijskem okolju. Po namestitvi na produkcijo, izvajalec preveri delovanje na enak način kot je bila narejena verifikacija na testnem okolju. Potrditveni test mora obsegati poleg delovanja same aplikacije tudi delovanje podatkovne zbirke in ustreznost baznih objektov.

5.6 Testiranje in zagotavljanje kakovosti

Razvojno okolje in testno okolje za razvojno testiranje izbrani izvajalec vzpostavi bodisi na svoji ali naročnikovi infrastrukturi. Prav tako izvajalec zagotovi uvoz podatkov za testiranje in šolanje testnih uporabnikov v testnem okolju kot tudi pripravo okolja za izvedbo šolanja uporabnikov.

Ker je ročno testiranje zamudno, riziko za napake pri izvajanju takšnih testov pa velik, se testiranje avtomatizira povsod kjer je to mogoče, kar omogoča ponovljivost. Zahteva se testno voden razvoj programskih rešitev, torej uporaba testov enot (angl. unit testing), po principu agilnega razvoja.

Osebe naročnika mora biti neposredno soudeleženo pri testiranju funkcionalnosti. Izvajalec za potrebe izvedbe prevzemnega testiranja s strani naročnika zagotovi orodje za prijavo in spremljanje napak (orodje mora biti uporabniku prijazno, omogočati mora opis napake, vstavljanje slik zaslonskih mask in pripenjanje dokumentov, kjer se je napaka pojavila ter spremljanje statusa odpravljanja evidentirane napake).

5.6.1 Načrt testiranja

Izvajalec pred začetkom testiranja pripravi in z naročnikom uskladi načrt testiranja funkcionalnosti. Načrt naj vsebuje:

- oceno števila preizkusnega osebja;
- krovni terminski načrt testiranja;
- oceno števila vseh primerov testiranj (use/test cases);
- izvajalčevo oceno glede potrebne kakovosti testnih podatkov za posamezne sklope testiranja (obstoječi produkcijski primeri, generirani primeri na podlagi produkcijskega algoritma, ročno sestavljeni primeri);
- grobo razdelitev tipov testiranj (testiranje posameznih primerov, testiranje posameznih uporabniških scenarijev);
- pravila dokumentiranja ugotovitev testiranja.

5.6.2 Testni scenariji in ugotovljene napake

Pred izvedbo testiranja je treba skladno z načrtom testiranja pripraviti testne scenarije. Tekom izvajanja testiranja je treba zabeležiti vse ugotovljene napake in neskladja glede na specifikacijo zahtev. Povzetek vseh ugotovljenih napak in neskladij se zabeleži v Poročilo o testiranju.

5.6.3 Testni scenarij

Testni scenarij je dokument, ki skladno z načrtom testiranja podrobneje predpisuje obliko in vsebino predvidenega testiranja.

Testni scenarij vsebuje:

- oznako funkcionalnosti, za katero se uporablja testni scenarij;
- naziv funkcionalnosti, za katero se uporablja testni scenarij;
- opis funkcionalnosti, za katero se uporablja testni scenarij;
- opis pogojev in zahtev za izvedbo testiranja po testnem scenariju;
- opis načrtovanega postopka izvedbe testiranja;
- opis pričakovanih rezultatov testiranja.

5.6.4 Poročilo o testiranju

Poročilo o testiranju mora vsebovati spodaj opisane podatke:

Splošni podatki o testiranju:

- oznaka in verzija izdelka, ki je bil predmet testiranja;
- konfiguracija strojne in programske opreme, ki je bila uporabljena pri izvedbi testiranja;
- navedena ali pripeta dokumentacija, ki je bila uporabljena kot podlaga za izvedbo testiranja.

Statistika ugotovljenih neskladnosti; za vsako testiranje je treba navesti:

- pregled ugotovljenih napak pri izvedbi testiranja;
- koliko napak je bilo odpravljenih in koliko je takih, ki so še v reševanju.

Rezultati testiranja:

Zahteve in priporočila v zvezi z dokumentacijo:

- predlog za dopolnitev dokumentacije s strani naročnika ali izvajalca.

Testiranje funkcionalnosti ter podatkov:

- rezultat izvedbe testov enot (angl. unit testing);
- opisi rezultatov testiranja;
- plan v zvezi z odpravo napak.

Zaključna ocena:

- zaključna ocena v zvezi s potekom in rezultati testiranja, ki mora vsebovati oceno ali je izdelek primeren za uvedbo v produkcijsko okolje ali ne.

5.7 Uporabniška in tehnična dokumentacija

Dokumentacija mora biti napisana v slovenskem jeziku.

5.7.1 Programska koda

Izvajalec naročniku preda celotno izvorno kodo z vsemi potrebnimi knjižnicami, da je mogoče neodvisno vzpostaviti delujoče razvojno okolje. Izvorno kodo je potrebno predati v obliki repozitorija, skladnega s splošno sprejetimi načini dela v industriji razvoja programske opreme (kot npr. GitHub, BitBucket...). Vse kasnejše nadgradnje in popravke izvorne kode je potrebno predati v isti repozitorij, tako da repozitorij vedno vsebuje zadnjo delujočo verzijo sistema ter po potrebi tudi testne verzije (module za test enot).

Za dele sistema, ki jih ni mogoče predati (npr. zaradi omejitev licenc) je potrebno natančno opisati, kako je mogoče manjkajoče dela sistema pridobiti in povezati s predano programsko kodo.

5.7.2 Tehnična dokumentacija - splošno

Izvajalec mora v okviru razvoja pripraviti tehnično dokumentacijo, ki vsebuje:

- opis zasnove in zgradbe sistema;
- opis vseh funkcionalnosti sistema z opisom delovanja;
- nabor in način integracije sistema z drugimi sistemi;
- opis protokolov za komunikacijo s sistemom z zahtevami glede varnosti in nadzora dostopa;
- opis protokolov za komunikacijo sistema z drugimi povezanimi sistemi s primeri.

5.7.3 Tehnična dokumentacija - namestitve

Izvajalec mora izdelati podrobna navodila za instalacijo in konfiguriranje celotnega sistema, opisati vse parametre za konfiguracijo predane programske opreme ter potrebne nastavitve podatkovnih baz,

pripravo podatkov in drugih sistemskih nastavitvev. Prav tako mora izdelati navodila za nameščanje posodobitev. Navodila naj zajemajo opis vzpostavitve testnega in produkcijskega okolja ter navodila za prehod iz testnega v produkcijsko okolje.

5.7.4 Uporabniška dokumentacija

Izvajalec mora izdelati navodila/priročnik za uporabnike in administratorje. Dokumentacija mora vsebovati vsaj:

- opis namena sistema in njegove glavne funkcionalnosti;
- vrste uporabnikov, ki jim je dokumentacija namenjena;
- varnostna navodila z osnovnimi smernicami za varno uporabo sistema, digitalnih potrdil, varovanje gesel in podatkov ter;
- podrobna navodila za uporabo vseh funkcij sistema.

Navodila za uporabo morajo vsebovati podroben opis uporabe aplikacij za posamezna vsebinska področja in postopke:

- Za vsak postopek so pripravljena podrobna navodila, kako naj uporabnik uporablja aplikacije.
- Navodila obsegajo celotno izvedbo postopka od prijave v sistem, zagona, izvedbe in zaključka procesa, do odjave iz sistema. Pri tem se naj navodila neposredno nanašajo (tudi grafično) na uporabniški vmesnik sistema.
- Poleg glavnega toka skozi proces mora dokumentacija pokriti tudi stranske tokove.
- Podani naj bodo razumljivi opisi vzrokov za vsa opozorila in napake, ki jih povzročajo uporabniške in/ali sistemske funkcije.
- Podana naj bodo podrobna navodila za programske vmesnike in konfiguracijo dostopa do sistema z uporabo programskih rešitev (vmesniki API).

Uporabniška dokumentacija mora uporabljati izrazoslovje poslovnega področja naročnika.

V uporabniški dokumentaciji je potrebno navesti kontaktno osebo ali naslov za pomoč pri morebitnih nejasnostih glede uporabe sistema.

Pri popravkih in nadgradnjah je potrebno zagotoviti posodabljanje vseh delov tehnične in uporabniške dokumentacije, ki morata ostati skladni s produkcijsko verzijo sistema.

5.8 Usposabljanje uporabnikov

V okviru aktivnosti usposabljanja ključnih uporabnikov mora izvajalec usposobiti ključne uporabnike naročnika za tehnično uporabo sistema.

Po izvedenem usposabljanju morajo biti udeleženci usposabljanja, ne glede na tip uporabnika, sposobni samostojno uporabljati posamezne funkcionalnosti sistema, ki so bile predmet usposabljanja.

Tako pripravo okolja kot tudi dokumentacijo za usposabljanje končnih uporabnikov in skrbnikov sistema, ki mora zajemati celovito gradivo, potrebno za obvladovanje snovi za izvedbo usposabljanj, zagotovi izvajalec.

6 Okvirni terminski načrt projekta

MEJNIKI

Vse aktivnosti morajo biti zaključene v 12 mesecih od podpisa pogodbe.

Mejnik M1 – Priprava projekta, do 2 meseca od podpisa pogodbe

A1. Izdelava podrobnega terminskega načrta za izvedbo javnega naročila

Mejnik M2 – Vzpostavitev sistema, do 10 mesecev od podpisa pogodbe

A2. Integracija podatkov NAP za potrebe C-ITS

A3. Izdelava spletnih vmesnikov za zunanje ponudnike informacij

A4. Izdelava scenarijev C-ITS

A5. Izdelava vmesnika BI centralne postaje C-ITS

A6. Izdelava vmesnika II centralne postaje C-ITS

A7. Integracija podatkov iz C-ITS v NAP

Mejnik M3 – Testiranje in prevzem celotnega sistema, do 12 mesecev od podpisa pogodbe

A8. Testiranje storitev nacionalnega vozlišča C-ITS in centralne postaje C-ITS

A9. Testiranje II in BI z drugimi nacionalnimi ali regionalnimi sistemi C-ITS

A10. Dokončni prevzem s poročilom in dokumentacijo ter predano izvorno kodo

Mejnik M4 – Vzdrževanje sistema, M3 + 36 mesecev od podpisa pogodbe

- Pogodbeno osnovno in dopolnilno vzdrževanje z mesečnim poročanjem in obračunom
- Zaključek pogodbe s poročilom o aktivnostih v garancijskem obdobju

Ob poteku vsakega mejnika izvajalec pripravi poročilo o delu.

7 Jamčevanje in vzdrževanje

7.1 Jamčevanje v garancijskem obdobju:

Po zapisniškem končnem prevzemu rešitve v produkcijsko okolje ob mejniku M4 sledi 36-mesečno garancijsko obdobje izdelanih produkcijskih rešitev.

Izvajalec jamči, da bo rešitev delovala v skladu s specifičnimi zahtevami in navodili za uporabo, v nasprotnem primeru bo v garancijskem obdobju brezplačno odpravil vse napake.

Napaka je definirana kot nedelovanje rešitve oziroma delovanje, ki ni v skladu z zahtevami, določenimi v končni specifikaciji zahtev, z zakonodajo oziroma tistimi, ki so z izvajalcem naknadno sporazumno dogovorjene, ali z navodili za uporabo rešitve. Napake se delijo glede na resnost, od česar je odvisna tudi hitrost oziroma nujnost odprave:

- kritična napaka: rešitev ne deluje v celoti ali ne delujejo njene ključne funkcionalnosti;
- resna napaka: rešitev deluje, a je delo oteženo in;
- manjša napaka: ne vpliva bistveno na funkcionalnost rešitve.

Odzivni čas na prijavo napake iz garancije po prejemu prijave je odvisen od narave napake. Odzivni čas je čas, ki preteče od prejema prijave napake do trenutka, ko izvajalec začne z odpravo napake. Izvajalec se zaveže napako odpraviti oziroma zagotoviti ustrezno funkcionalno nadomestno rešitev tako, da bo delovni proces uporabnika nemoten.

Narava (kategorija) napak, odzivni časi in čas odprave napak je podan v spodnji preglednici:

Tabela 1. Kategorije napak, odzivni časi in časi odprave napak.

Kategorija	Odzivni čas	Čas odprave
Kritična napaka	1 ura	neprekinjena intervencija do odprave napake
Resna napaka	4 ure	intervencija do odprave napake
Manjša napaka	16 ur	intervencija do odprave napake z možnimi prekinitvami po pisnem dogovoru z naročnikom

Navedeni časi veljajo za poslovni čas NCUP v režimu 24/7. Če izvajalec po pregledu prijave napake ugotovi, da bo za njeno odpravo potrebno več kot 24 h, je dolžan to pisno sporočiti naročniku in za vmesni čas vzpostaviti ustrezno funkcionalno nadomestno rešitev tako, da bo delovni proces uporabnika nemoten.

Izvajalec ni odgovoren za napako, ki je nastala kot posledica:

- naročnikovega neupoštevanja navodil za uporabo oziroma uporabniške dokumentacije;
- naročnikove nestrokovne, nepravilne ali nedovoljene uporabe rešitve oziroma operacijskega sistema okolja oziroma računalniške strojne opreme;
- nedovoljenih modifikacij rešitve s strani naročnika ali tretjih oseb, in;
- višje sile, nesreče in podobnih nepredvidljivih dogodkov ali malomarnosti, za kar ni odgovoren izvajalec.

Jamčevalni rok se podaljša za čas, ki ga izvajalec potrebuje za odpravo javljene mu bistvene napake (kritične oziroma resne napake).