

Příloha č. 1 Smlouvy o dodávce hardware a software a poskytnutí souvisejících služeb – Technická specifikace

(dále jen „Technická specifikace“)

I. ÚVOD

1. Dodávka spadá do oblasti moderních technologií v podobě nové generace ITS systémů – tzv. kooperativních inteligentních dopravních systémů (C-ITS). Tyto systémy jsou založeny na vzájemné komunikaci V2X, tzn. mezi vozidlem a infrastrukturou, popř. mezi vozidly navzájem. V rámci této komunikace dochází k obousměrné výměně dat mezi jednotkami umístěnými ve vozidlech (OBU) a jednotkami na infrastruktuře (RSU), přičemž je využíváno specifické bezdrátové technologie operující na frekvenci 5,9 GHz. Toto frekvenční pásmo bylo celosvětově vyhrazeno pro bezpečnostní aplikace v dopravě. V rámci této komunikace se využívá standard IEEE 802.11p, který byl v Evropě dále rozpracován do podoby standardu ITS-G5. Nad rámec ITS-G5 se pro přenos dat v C-ITS využívá také stávajících datových sítí mobilních operátorů. Systémy, které využívají jak ITS-G5, tak veřejné mobilní sítě, se nazývají „hybridní“.
2. Dodávka bude realizována v kontextu víceletého mezinárodního projektu C-ROADS, který je spolufinancován z evropského dotačního programu CEF (Connecting Europe Facility). C-ROADS je aktivita běžící paralelně v 18 evropských zemích, přičemž jejím cílem je zavádění vzájemně interoperabilních C-ITS služeb na evropských silnicích, dálnicích a ve městech. Za tímto účelem vznikla mezinárodní C-ROADS Platforma (www.c-roads.eu), jejímž hlavním úkolem je zajištění interoperability technických a funkčních řešení v jednotlivých státech tak, aby řidič při překročení hranic dostával stejně kvalitní a srozumitelnou službu, jako v jeho domovské zemi. Výstupy této platformy jsou reflektovány i ve specifikacích této dodávky. V tomto kontextu vznikl v ČR projekt C-ROADS Czech Republic (www.c-roads.cz), který je koordinován Ministerstvem dopravy a který má za úkol v období 2016 – 2020 systematicky implementovat C-ITS systémy a poskytovat související služby na vybraných českých dálnicích, silnicích I. třídy, ve městech a na železničních přejezdech. Tyto systémy budou realizovány na základě společných specifikací, které reflektují výstupy C-ROADS Platformy a další specifické požadavky zainteresovaných subjektů.
3. Zadavatel jakožto člen řešitelského konsorcia projektu C-ROADS Czech Republic vypisuje tuto zakázku, jejímž cílem je zajištění nezávislého testování implementací dalších partnerů a zajištění souladu se specifikacemi C-ROADS Platformy (WG2 a WG3) a C-ROADS Czech Republic v rámci jednotlivých realizací:
 - 3.1. DT1 – Implementace C-ITS systému na D1 km 190 – 210, odpovědný partner projektu je Ředitelství silnic a dálnic ČR
 - 3.2. DT2 – Implementace C-ITS systému ve městě Brně, odpovědný partner projektu jsou Brněnské komunikace a.s.
 - 3.3. DT3 – Implementace C-ITS systému na dálnicích D5 km 20 – 90 a D11 km 1 – 90, odpovědný partner projektu je Ředitelství silnic a dálnic ČR

- 3.4. DT4 – Implementace C-ITS systému na vozidlech MHD ve městech Ostrava a Plzeň, odpovědným partnerem projektu je INTENS Corporation s.r.o.
 - 3.5. DT5 – Implementace C-ITS systému na železničních přejezdech, odpovědný partner projektu je Správa železniční dopravní cesty, s.o. a AŽD Praha a.s.
 - 3.6. DT6 – Přeshraniční testování
4. Z tohoto důvodu bude kladen zvláštní důraz na dodržení technických a funkčních specifikací na dodané řešení, neboť je nutné zajistit soulad s mezinárodními specifikacemi za účelem zachování interoperability napříč Evropou. V průběhu plnění zakázky se předpokládá úzká spolupráce Dodavatele s konsorciem projektu C-ROADS Czech Republic, které bude dohlížet právě na plnění definovaných požadavků.

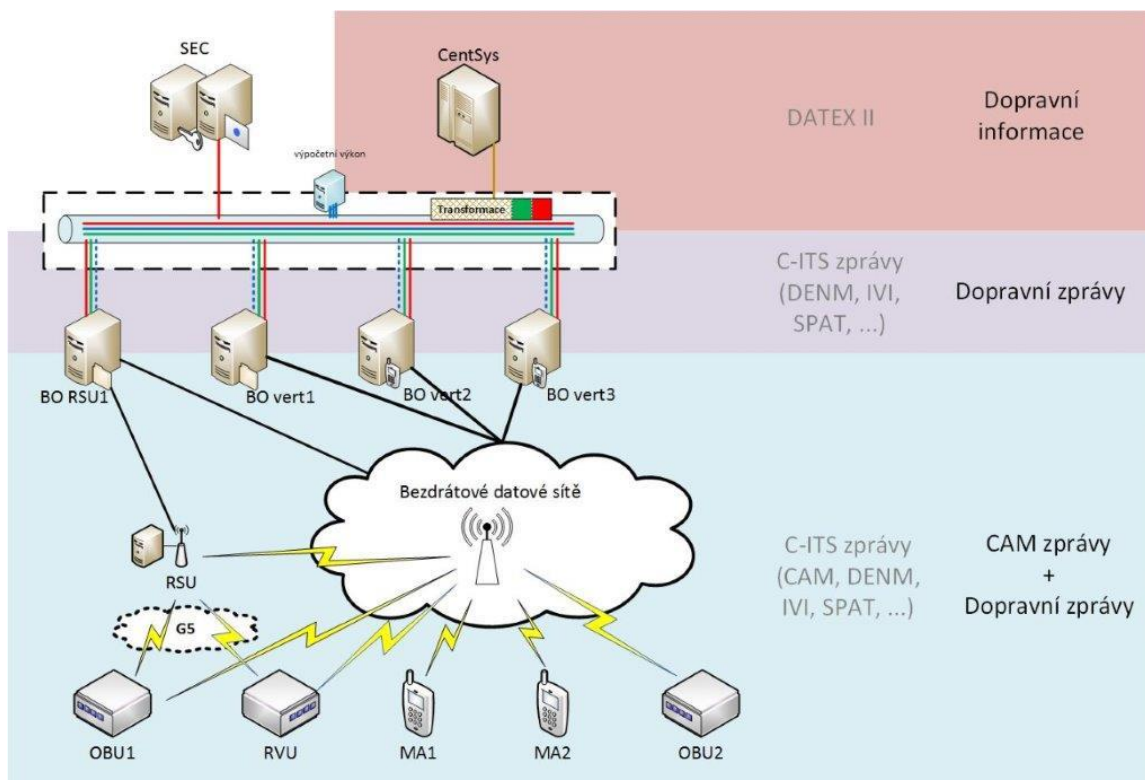
II. PŘEDMĚT VEŘEJNÉ ZAKÁZKY

1. Předmět veřejné zakázky vychází z potřeby Zadavatele vybudovat funkční systém umožňující nezávislé testování funkčnosti C-ITS komponent nebo celých systémů v rámci realizace dílčích implementací v rámci projektu C-ROADS Czech Republic. Tato veřejná zakázka se skládá z dodávky hardwarových a softwarových komponent a zajištění provozu a podpory systému a testování nejdéle do 30.11.2020, detailní popis je uveden dále v textu.
2. Základní části dodávky jsou:
 - 2.1. Dodávka SW licence pro testovací nástroj „C-ITS SIM“ vč. licence pro SW stack.
 - 2.2. Dodávka příslušných SW licencí pro aplikační logiku na C-ITS jednotky.
 - 2.3. Dodávka mobilního PC (laptop) vč. operačního systému LINUX nebo Windows 10.
 - 2.4. Dodávka 2 ks C-ITS hybridních jednotek umožňující v nastavení použití jako OBU nebo RSU jednotky a jejich integrace do C-ITS SIM, tyto jednotky musí umožnit komunikaci pomocí ITS-G5 a LTE. Tato dodávka bude vč. příslušného SW stacku.
 - 2.5. Služby spojené s provedením funkčních integrací C-ITS SIM na Integrační Platformu projektu C-ROADS Czech Republic.
 - 2.6. Služby spojené s provedením funkčních integrací C-ITS SIM a 2ks C-ITS hybridních jednotek na PKI infrastrukturu.
 - 2.7. Služby spojené s provedením funkční integrace OBU/RSU jednotek do nástroje C-ITS SIM.
 - 2.8. Služby spojené s testováním Zadavatelem požadovaných scénářů v rámci C-ROADS Czech Republic a pilotního ověření v rozsahu max. 100 člověkodní.
 - 2.9. Proškolení 3 členů týmu Zadavatele pro používání a administraci dodaného SW a HW.
 - 2.10. Služby podpory a provozu systému dle požadavků této ZD nejdéle do 30.11.2020.
3. Předmětem veřejné zakázky není:
 - 3.1. Dodávka Integrační platformy
 - 3.2. Dodávka PKI infrastruktury
 - 3.3. Tyto činnosti související s touto dodávkou budou zajištěny Zadavatelem, popř. jinými subjekty v průběhu realizace této dodávky.

III. ARCHITEKTURA PROJEKTU C-ROADS CZECH REPUBLIC

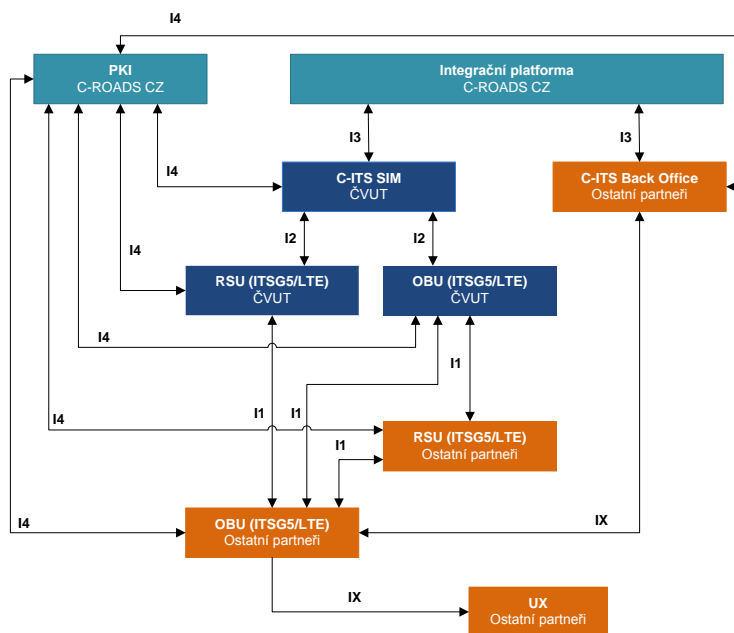
1. V této části je popsána obecná architektura budoucího C-ITS systému realizovaného pro potřeby Zadavatele včetně jeho jednotlivých komponent na úrovni centrálních systémů, infrastruktury i vozidel. Některé komponenty budou dodány v rámci této dodávky, zatímco jiné již byly nebo jsou budovány v rámci jiných projektů.
2. Architektura C-ITS systému vychází ze specifikací vytvořených v rámci projektu C-ROADS Czech Republic (Příloha č. 2 Smlouvy o dodávce hardware a software a poskytnutí souvisejících služeb) a také z obdobných systémů budovaných v zahraničí v rámci platformy C-ROADS. Schéma je znázorněno na Obr. 1. Systém je rozdělen do následujících základních vrstev, kde se nacházejí konkrétní fyzické i komunikační prvky:
 - 2.1. **Centrální systémy.** Centrální systémy jsou základní částí systému C-ITS založené na prvcích umožňujících příjem, zpracování, generování a distribuci C-ITS zpráv. Mezi prvky centrálních systémů patří:
 - a) C-ITS back office (C-ITS BO) – je typicky realizován partnery projektu, kteří generují a zpracovávají C-ITS zprávy.
 - b) Integrovaná platforma (IP) – specifický prvek v rámci projektu C-ROADS Czech Republic pro výměnu informací mezi C-ITS BO jednotlivých partnerů. IP byla realizována v rámci projektu C-ROADS Czech Republic a Dodavatel v rámci této dodávky zajistí připojení testovacího nástroje C-ITS SIM k této platformě.
 - c) PKI infrastruktura (PKI) – prvky zajišťující bezpečnost dat a komunikace v rámci celého ekosystému C-ROADS Czech Republic. Systém PKI byl vybudován partnery projektu C-ROADS Czech Republic na komerčním bezpečnostním řešení TeskaLabs SeaCat¹. Dodavatel v rámci této dodávky zajistí součinnost při napojení testovacího nástroje C-ITS SIM a dodávaných C-ITS jednotek k PKI infrastruktuře a využívání jeho funkcionalit.
 - 2.2. **Komunikační síť.** Jedná se o přenosové vrstvy zajišťující komunikaci mezi C-ITS BO a/nebo testovacím nástrojem C-ITS SIM a C-ITS jednotkami (OBU/RSU). V článku VII jsou popsány základní komunikační rozhraní mezi jednotlivými prvky systému. Přenosové cesty v rámci C-ITS systému lze rozdělit do třech základních kategorií:
 - a) pevné sítě (optické či metalické);
 - b) veřejné sítě mobilních operátorů;
 - c) mikrovlnná DSRC technologie pracující ve frekvenčním pásmu 5,9 GHz a využívající mezinárodně uznávaný standard ITS-G5.
 - 2.3. **Infrastruktura / vozidlo.** V této vrstvě se nacházejí RSU/OBU jednotky instalované buď na dopravní infrastruktuře, nebo ve vozidle. Díky požadavku na možnost nastavení jednotky jako RSU nebo OBU je možno OBU jednotku ve vozidle upravit na RSU jednotku a obráceně. To znamená, že stojící vozidlo se může dočasně změnit na statickou RSU jednotku. V obou případech bude možné propojit tyto jednotky s testovacím nástrojem C-ITS SIM.

¹ Popis produktu je dostupný na <https://docs.teskalabs.com/seacat/resources/c-its/>



Obr. 1 Architektura C-ITS řešení C-ROADS Czech Republic

3. Schéma na Obr. 2 zobrazuje typický C-ITS systém budovaný v rámci C-ROADS Czech Republic se zvýrazněním částí (modře), které jsou součástí této dodávky a jeho vazby na externí stávající či nově budované prvky. Ve schématu jsou označena také jednotlivá rozhraní, která jsou dále popsána v článku VII. Díky požadavku Zadavatele na provádění nezávislých testů pro všechny partnery projektu C-ROADS Czech Republic a jejich implementace C-ITS systémů je nezbytné, aby dodávané řešení sloužilo jako „etalon“ pro testování na národní a popř. mezinárodní úrovni. To znamená, že Dodavatel bude schopný provést nezbytné SW úpravy na C-ITS SIM nástroji tak, aby zohlednil použití konkrétních sad norem (tzv. profiling tj. implementace vybraných norem a jejich konkrétních verzí; je nutné zdůraznit fakt, že ne všechny verze norem jsou zpětně kompatibilní, což může způsobovat technickou nekompatibilitu vysílaných ITS zpráv) a nastavení systému odpovídající implementaci konkrétního projektového partnera a v rámci poskytovaných služeb umožnil nezávislé testování funkčnosti.



Obr. 2 Schéma typického C-ITS systému v rámci C-ROADS Czech Republic

IV. POPIS C-ITS SLUŽEB TÝKAJÍCÍCH SE DODÁVKY

1. Tato část je zaměřena na popis základních C-ITS služeb (tzv. Use Case nebo také UC), které budou předmětem dodávky a jejichž ověření dodávaný testovací nástroj C-ITS SIM musí umožnit. Cílovými skupinami těchto služeb bude primárně Zadavatel a partneři projektu C-ROADS Czech Republic.
2. Primárním cílem dodávky je zajištění prostředí a podmínek k nezávislému testování všech služeb a funkčnosti systémů budovaných jednotlivými projektovými partnery v rámci projektu C-ROADS Czech Republic.
3. Níže jsou popsány jednotlivé C-ITS služby, které jsou předmětem plnění této dodávky. Detailní popis a požadavky na jednotlivé služby vycházejí ze specifikací vytvořených v rámci projektu C-ROADS Czech Republic a mezinárodní C-ROADS Platformy a jsou uvedeny v Příloze č. 2 Smlouvy o dodávce hardware a software a poskytnutí souvisejících služeb. Jednotlivé C-ITS služby lze rozdělit do dvou skupin.
 - 3.1. **Kompletní implementace C-ITS služby.** V této skupině se nacházejí UC, u nichž se v rámci této dodávky vyžaduje kompletní implementace, tzn. tvorba C-ITS zpráv dle ETSI/ISO standardů pro konkrétní UC, možnost modifikace této C-ITS zprávy a zajištění vyslání C-ITS zprávy pomocí RSU nebo OBU jednotky pomocí ITS-G5. Pro tyto účely je nezbytné, aby C-ITS zprávy byly generovány na testovacím nástroji C-ITS SIM a současně byly provedeny úpravy a nastavení na samotných C-ITS jednotkách (OBU/RSU), se kterými budou komunikovat C-ITS jednotky třetích stran. Jedná se o následující služby (UC):
 - a) vozidlo jako sonda v dopravním proudu (Probe Vehicle Data - PVD);
 - b) upozornění na nepříznivé povětrnostní podmínky (Weather Conditions Warning-WCW);

- c) upozornění na (dočasné) práce na silnici (Road Works Warning - RWW);
- d) upozornění na nebezpečné místo (Hazardous Location Notification - HLN);
- e) upozornění na pomalu jedoucí nebo stojící vozidlo (Slow and Stationary Vehicle - SSV);
- f) zobrazení dopravních informací přímo ve vozidle (In-Vehicle Information - IVD);
- g) upozornění na blížící se dopravní kongesci (Traffic Jam Ahead - TJA).

3.2. **Interpretace C-ITS zpráv v testovacím nástroji C-ITS SIM.** V této skupině se nacházejí UC, jejichž C-ITS zprávy dle ETSI/ISO standardů musejí být interpretovány na testovacím nástroji C-ITS SIM (tzn., musejí být schopny zobrazit notifikaci na displeji mobilního PC), resp. OBU jednotka ve vozidle musí být schopna tyto zprávy přijímat, zpracovat a předat je k zobrazení do C-ITS SIM. Tyto zprávy se mohou dostat do C-ITS SIM z Integrovaných platformy nebo z RSU/OBU jednotek implementovaných třetími stranami. C-ITS zprávy této skupiny UC však nemusí RSU/OBU ani C-ITS SIM umět generovat, pokud není řečeno jinak. Jedná se o následující služby:

- a) nerespektování návěstí světelného signalizačního zařízení na křižovatce (Intersection Signal Violation – ISV);
- b) upozornění na blížící se vozidlo IZS (Emergency Vehicle Approaching – EVA);
- c) upozornění na prudce brzdící vozidlo (Electronic Emergency Brake Light – EEBL);
- d) přednost vozidlu veřejné osobní dopravy (Public Transport Priority – PTP);
- e) upozornění na úrovně železniční přejezd ve výstražce (Railway Level crossing – RLX);
- f) upozornění na přibližující se tramvaj k technicky nezabezpečenému tramvajovému přejezdu (Public Transport Safety – PTS);
- g) bezpečnost vozidel veřejné osobní dopravy (např. dání přednosti v jízdě vozidlu MHD při vyjíždění z vyhrazeného jízdního pruhu, upozornění na vystupující cestující v tramvajové zastávce s výstupem do vozovky) (Public Transport Safety – PTS).

V. OBECNÉ TECHNICKÉ POŽADAVKY KLADENÉ NA SOFTWAREVÝ NÁSTROJ C-ITS SIM

1. V rámci této dodávky Dodavatel vyvine a dodá softwarový nástroj C-ITS SIM určený pro vyhodnocování funkčnosti C-ITS systémů či jejich dílčích prvků. V tomto C-ITS SIM se koncentrují všechna důležitá data, která se dle jasných pravidel dále distribuují do prvků na nižších úrovních C-ITS systému (RSU/OBU), popř. do nadřazených systémů (PKI/IP). Komunikace C-ITS SIM se všemi prvky C-ITS systému probíhá obousměrně.
2. Dodavatel musí dodat C-ITS SIM jako rozšiřitelný systém, který bude připraven na budoucí úpravy (o další C-ITS služby a/nebo modifikace na základě změny standardů) a současně umožní propojení s externími systémy jako např. připojení k PKI infrastruktury nebo

Integrační platformě. C-ITS SIM dále umožní přímé propojení a integraci s C-ITS jednotkami (OBU/RSU).

3. C-ITS SIM bude umožňovat obousměrnou komunikaci s:
 - 3.1. **Integrační platformou**, detailní specifikaci rozhraní (I3 viz článek VII) předá Zadavatel Dodavateli v průběhu realizace dodávky. Tato komunikace zajistí výměnu C-ITS zpráv (DENM, IVI) s C-ITS back offices třetích stran a dojde tak k možnosti ověření správnosti vysílaných C-ITS zpráv.
 - 3.2. **PKI infrastrukturou** fungující na technologii TeskaLabs SeaCat, detailní specifikaci rozhraní (I4 viz článek VII) předá Zadavatel Dodavateli v průběhu realizace dodávky. Tato komunikace zajistí integraci s certifikačními autoritami Root CA, Enrolment CA a Authorization CA projektu C-ROADS Czech Republic.
 - 3.3. **RSU / OBU jednotkami** umístěnými ve vybraných vozidlech Zadavatele (viz článek VIII). Komunikace bude zajištěna prostřednictvím rozhraní I2 definovaném v článku VII. Tato komunikace bude zajištěna pomocí pevného kabelového spojení (Ethernet, RS 232 nebo obdobné) a současně umožní také LTE spojení mezi C-ITS jednotkami a C-ITS SIM a bude umožňovat výměnu C-ITS zpráv.
4. C-ITS SIM bude dodán jako ucelená funkční SW aplikace, která bude instalovaná na dodané mobilní PC a umožní funkcionality popsané dále v této technické specifikaci.

VI. FUNKČNÍ POŽADAVKY KLADENÉ NA C-ITS SIM

1. V této části technické specifikace jsou popsány funkční požadavky a hlavní funkcionality softwarového nástroje C-ITS SIM.
2. **Testovací scénáře.** C-ITS SIM musí umožnit testování jednotlivých scénářů a UC (definovaných v článku IV) a specificky pak podporovat následující funkcionality:
 - 2.1. Analýza přijatých zpráv z ITS-G5.
 - 2.2. Analýza přijatých zpráv z Integrační Platformy.
 - 2.3. Odeslání zpráv do IP a ověření příjmu přes ITS-G5 (např. v místě umístění RSU).
 - 2.4. Odeslání zprávy do IP a ověření příjmu přes LTE pomocí proprietární aplikace testovaného subjektu.
3. **Příjem C-ITS zpráv.** C-ITS SIM spolu s připojenou C-ITS jednotkou, která je součástí dodávky, musí umožnit Zadavateli následující aktivity:
 - 3.1. Provádět záchyt zpráv přijatých z ITS-G5 v binárním formátu (PCAP) na místě měření v terénu na dodaných OBU jednotkách.
 - 3.2. Možnost ověření struktury jednotlivých paketů a jejich soulad s C-ITS normami (CAM, DENM, IVI, SPAT-MAP, SSM/SRM).
 - 3.3. Umožnit konverzi ITS zprávy z ASN.1 formátu do textové formy.
 - 3.4. Interpretace C-ITS zprávy a převod na konkrétní Use case z katalogu projektu C-ROADS Czech Republic.

- 3.5. Označení a logování zpráv, jejichž interpretace se nezdařila pro pozdější analýzu, tj. analýzu „nehodných“ (špatně vyplněných) zpráv, které neodpovídají platným C-ITS normám.
- 3.6. Obdobná analýza pro všechny zprávy přijaté z Integrované Platformy, vypracování základních statistik procentuální úspěšnosti při interpretaci zpráv od každého subjektu připojeného do IP.
4. **Odesílání C-ITS zpráv.** C-ITS SIM spolu s připojenou C-ITS jednotkou musí umožnit Zadavateli odesílání C-ITS zpráv. Jedná se o funkce zajišťující tvorbu C-ITS zpráv pro konkrétní Use Case, komunikaci mezi C-ITS SIM a C-ITS jednotkami (OBU/RSU). Hlavním úkolem C-ITS SIM, kromě vlastní komunikace s jednotkami, je převod zpráv mezi MQTT/XML reprezentací používanou směrem k C-ITS jednotkám (definovanou v rozhraní I2 v článku VII) a objektovou reprezentací používanou v C-ITS SIM při komunikaci s ostatními moduly. To znamená dodání následujících funkcionalit:
 - 4.1. Vytvoření nástroje, který opakovaně odesílá zvolený typ C-ITS zprávy do ITS-G5 a do Integrované platformy. Při opakovaném odeslání bude zpráva identická s výjimkou časových údajů označujících dobu její platnosti
 - 4.2. Logování odeslaných zpráv pro pozdější srovnání se zprávami přijatými na testovací straně.
 - 4.3. Možnost uložení nadefinovaných scénářů a jejich opětovné nahrání s možností změny času platnosti.
5. **Komunikace C-ITS jednotek s C-ITS SIM.** Komunikace mezi klíčovými komponentami C-ITS jednotkami a C-ITS SIM bude založena na protokolu TCP/IP. Při komunikaci s OBU jednotkami je tento modul v komunikaci vždy serverem, OBU jednotky budou vždy klienty. Komunikace je zabezpečená pomocí VPN, popř. dedikované APN v případě komunikace přes veřejné sítě mobilních operátorů.
6. Pro účely této implementace a požadovaných Use cases (definovaných v článku IV) budou z C-ITS SIM směrem k C-ITS jednotkám rozesílány DENM a IVI zprávy a současně budou přijímány od C-ITS jednotek DENM, IVI, SPAT-MAP, CAM a SSM/SRM zprávy a data pro další zpracování.
7. C-ITS SIM musí zajistit veškeré zpracování a třídění všech dopravních informací a tvorbu odpovídajících C-ITS zpráv, a to v obou směrech, tj. na IP i na připojená zařízení C-ITS systému. Součástí C-ITS SIM je i validace a porovnávání dostupných dat. Modul také zajistí distribuci zpráv do konkrétních C-ITS jednotek.
8. C-ITS SIM umožní sledovat stavy všech zařízení v systému, vytvářet odpovídající stavové informace, ukládat je pro potřeby analýzy historických dat a přímé zobrazení v GUI.
9. **Uživatelské rozhraní (GUI).** Uživatelské rozhraní bude zajišťovat interakci C-ITS SIM s jeho uživateli, a to formou (i) srozumitelného předávání informací vzniklých v C-ITS systému směrem k uživateli a (ii) jednoduchého zadávání vstupních parametrů uživatelem do C-ITS SIM. GUI bude zajišťovat minimálně následující funkcionalitu:
 - 9.1. Zobrazování aktuálních událostí – na mapovém podkladu budou zobrazovány aktuální události z C-ITS systému, které je možné dále filtrovat, třídít či zobrazovat v seznamu. Dispečer bude mít možnost tyto události editovat či zrušit (viz další funkce).
 - 9.2. Manuální tvorba událostí – dispečer musí mít možnost manuálně zadat v mapě novou událost (nehoda, stojící vozidlo, práce na silnici, dojezdové doby), popř. editovat

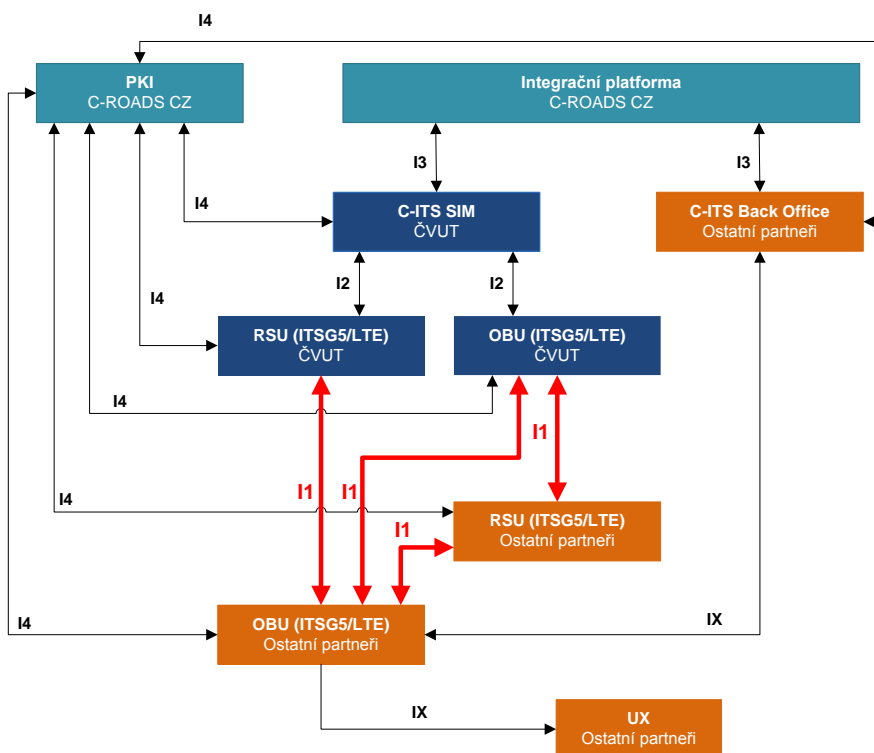
- stávající události – měnit či přidávat dodatečné parametry (např. rychlostní omezení u prací na silnici).
- 9.3. Mapové podklady – základem GUI jsou kvalitní a aktuální mapové podklady pokrývající minimálně oblasti pilotních projektů realizovaných v rámci projektu C-ROADS Czech Republic. V mapě budou zobrazeny minimálně následující objekty:
 - a) kompletní silniční a uliční síť;
 - b) poloha mobilních jednotek (OBU);
 - c) aktuálně vysílané události.
 - 9.4. Zobrazování archivovaných informací – operátor musí mít možnost procházet archivované záznamy, tj. minimálně přijaté a odeslané zprávy, chybová hlášení a systémové a provozní zprávy.
 - 9.5. Správa zařízení – uživatelské rozhraní musí umožňovat sledovat stavy a funkci připojených zařízení (OBU/RSU), která jsou zapojena do C-ITS SIM aplikace. RSU/OBU zařízení se budou na mapovém podkladu zobrazovat v barevném rozlišení podle svého aktuálního stavu (Online/porucha jednotky, resp. její komponenty/Offline). Po „rozkliknutí“ ikony daného zařízení se budou v detailu zařízení zobrazovat alespoň následující informace (některé položky jsou relevantní pouze pro vozidlové jednotky):
 - a) ID jednotky;
 - b) Typ/model zařízení a verze firmware;
 - c) označení ulice/pozemní komunikace, na které se jednotka nachází (popř. křižujících ulic);
 - d) zásobník vysílaných informací (DENM, IVI, CAM);
 - e) vizualizace stavu jednotlivých komponent systému;
 - f) typ vozidla;
 - g) kategorie vozidla;
 - h) vybrané stavové informace o periferních systémech vozidla (stav majáku);
 - i) čas posledního spojení.
 - 9.6. Dále musí být možno prostřednictvím GUI vykonávat následující funkce:
 - a) aktivace/deaktivace jednotky.
 - 9.7. Správa uživatelů – v GUI musí být administrační sekce, která bude obsahovat správu uživatelů, kteří mají přístup k jednotlivým funkcím a úrovním C-ITS SIM. V této části je možné nastavovat přístupová práva pro jednotlivé role i konkrétní uživatele. Minimálně budou definovány 2 role uživatelů:
 - a) administrátor – s plným přístupem;
 - b) operátor – s omezeným přístupem;
 - 9.8. Detailní specifikace jednotlivých rolí bude upřesněna v průběhu realizace.
10. C-ITS SIM musí umožnit integraci a poskytování kryptografických služeb, kde se jedná především o podepisování odchozích zpráv v místě C-ITS SIM, ověřování validity přijatých

zpráv, resp. elektronických podpisů, šifrování a dešifrování uživatelského obsahu (payloadu), správa certifikátů, zpracování CRL, CTL atp.

11. Security modul bude integrován s PKI infrastrukturou C-ROADS Czech Republic fungující na technologii TeskaLabs SeaCat, a to zejména s Root CA, Enrolment CA a Authorization CA (viz článek X).
12. Základní předpokladem implementace security řešení je, že veškeré operace s kryptografickým materiálem musí probíhat pouze v zabezpečeném hardwarovém zařízení splňujícím bezpečnostní vlastnosti Common Criteria EAL 4+ (tzv. Hardware Security Module - HSM), čímž bude eliminováno riziko jeho kompromitace.

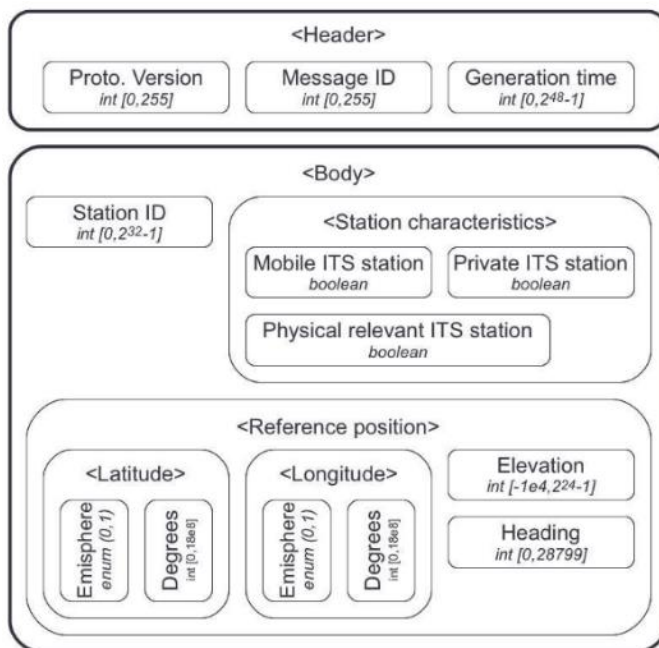
VII. KOMUNIKAČNÍ ROZHŘANÍ

1. Mezi jednotlivými prvky C-ITS systému jsou definována rozhraní, která mají své specifické požadavky. Pro komunikaci krátkého dosahu mezi OBU a RSU (popř. mezi OBU navzájem) je vyhrazeno pásmo 5,9 GHz dle specifikací ITS-G5.
2. Ostatní rozhraní v rámci C-ITS systému jsou v zásadě dvojího typu – realizovaná prostřednictvím pevného spojení (Ethernet s využitím optických či metalických kabelů) a dále rozhraní využívající bezdrátové sítě mobilních operátorů. V C-ITS systému byla definována tato rozhraní, která jsou následně podrobněji popsána:
 - 2.1. Rozhraní I1: RSU/OBU ↔ RSU/OBU
 - 2.2. Rozhraní I2: C-ITS SIM ↔ RSU/OBU
 - 2.3. Rozhraní I3: C-ITS SIM ↔ Integrovaná platforma.
 - 2.4. Rozhraní I4: C-ITS SIM/RSU/OBU ↔ Centrální PKI server.
3. **Rozhraní I1: vozidlové jednotky ↔ jednotky na infrastruktuře/vozdlové jednotky.** Komunikace mezi jednotkou na infrastruktuře a vozidlovou jednotkou je základním principem C-ITS systému. V rámci tohoto spojení se periodicky obousměrně vyměňují informace o stavu příslušných jednotek pomocí mikrovlnné technologie DSRC. Pro toto spojení bylo celosvětově vyhrazeno frekvenční pásmo 5,9 GHz, ve kterém probíhá rádiová komunikace krátkého dosahu. Výhodou této technologie je její rychlost a spolehlivost, přičemž výměna informací může probíhat až desetkrát za vteřinu. Schéma na Obr. 3 zobrazuje architekturu umístění a napojení na rozhraní I1 pro budovaný C-ITS systém.



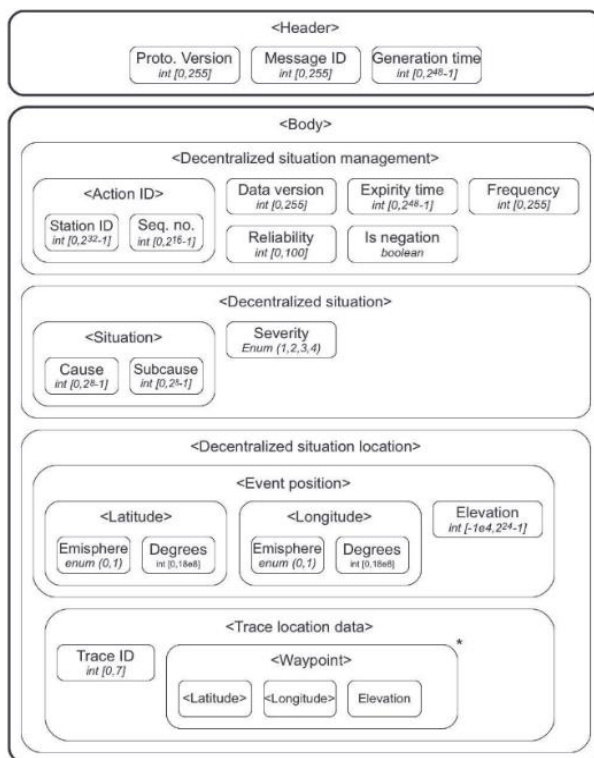
Obr. 3 Architektura umístění a napojení rozhraní II

4. Komunikace mezi vozidlovými jednotkami a jednotkami na infrastruktuře, popř. mezi dvěma vozidlovými jednotkami navzájem, byla na mezinárodní úrovni standardizována. Příslušný standard v Evropě je označován jako ITS-G5, vychází ze standardu IEEE 802.11p a je definován v normách ETSI. Konkrétně se jedná o následující dokumenty:
 - 4.1. ETSI ES 202 663 – European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band
 - 4.2. ETSI EN 302 663 – Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
 - 4.3. ETSI TS 102 637 – Vehicular Communications; Basic Set of Applications
5. Ve výše uvedených předpisech jsou definovány základní typy zpráv, které jsou v rámci standardu ITS-G5 generovány a posílány, jedná se o zprávy CAM, DENM, IVI, SPAT a MAP, které jsou dále podrobněji popsány:
 - 5.1. **Cooperative Awareness Message (CAM).** Zprávy CAM jsou generovány a odesílány periodicky až 10x za sekundu dle okolních podmínek. Poskytují základní informace o zařízení, které je vygenerovalo (OBU jednotka). Obsahují hlášení o přítomnosti, poloze, teplotě a provozním stavu příslušného zařízení. Zprávy CAM jsou mimo jiné využívány pro výpočty dojezdových dob, zdržení, průměrných rychlostí apod. v rámci služby Probe vehicle data. Zprávy CAM přijímají také ostatní OBU jednotky v okolí „vysílající jednotky“. Specifikace zprávy CAM je detailně popsána v předpisu *ETSI TS 102 637-2 Specification of Cooperative Awareness Basic Service*. Jednotlivé atributy zprávy CAM jsou popsány ve standardu *ETSI TS 102 894-2 Applications and facilities layer common data dictionary*. Struktura zprávy CAM je znázorněna na Obr. 4.



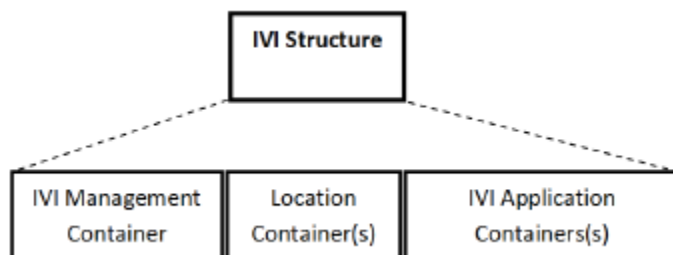
Obr. 4 Struktura zprávy CAM

- 5.2. **Decentralized Environmental Notification Message (DENM).** Zprávy DENM jsou generovány pouze v případě výskytu nějaké události, jejich odeslání tedy musí přecházet nějaký spouštěč. Pomocí DENM zpráv se tedy přenášejí informace o mimořádných událostech, jako je práce na silnici, dopravní nehoda, kluzká vozovka, jízda v protisměru či jiný typ překážky atp. Zpráva může být generována v C-ITS back office, popř. přímo v OBU jednotce. RSU jednotky zprávy DENM pouze preposílají do vozidel ve svém dosahu či naopak do C-ITS back office dle typu události. Zprávy DENM jsou vysílány periodicky, dokud je příslušná událost platná. K přerušení vysílání dojde buď v případě, že vyprší její přednastavená doba platnosti, nebo příslušná C-ITS jednotka vyšle speciální DENM zprávu, která zruší platnost dotčené události. Specifikace zprávy DENM je detailně popsána ve standardu *ETSI TS 102 637-3 Specification of Decentralized Environmental Notification Basic Service*. Jednotlivé atributy zprávy DENM jsou popsány ve standardu *ETSI TS 102 894-2 Applications and facilities layer common data dictionary*. Struktura DENM zprávy je znázorněna na Obr. 5.



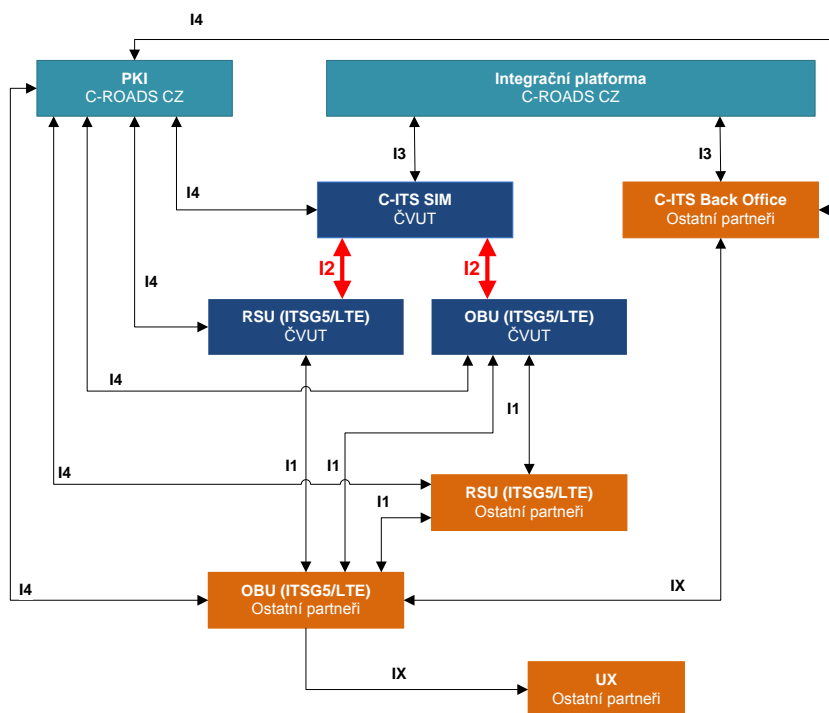
Obr. 5 Struktura zprávy DENM

- 5.3. **In-Vehicle Information (IVI).** Zprávy IVI obecně slouží primárně pro přenos informací o statických a dynamických dopravních symbolech, např. dopravní symboly na portálech liniového řízení dopravy (LŘD), informačních portálech (ZPI/PDZ) a zařízeních pro provozní informace (ZPI), do vozidla nebo do HMI zařízení. IVI zpráva je generována přímo v C-ITS back office a je následně odeslána do příslušné RSU jednotky v blízkosti daných portálů. RSU jednotky dále zprávu IVI přeposílají do vozidel ve svém dosahu. IVI zpráva neslouží pouze pro přenos zobrazovaných dopravních symbolů, ale také doplňkových textů (informační portály ZPI/PDZ). Získané informace jsou následně HMI zařízením ve vozidle vhodně prezentovány řidiči dle knihovny dopravních symbolů a typického rozložení dopravních značení na portálech. Zpráva IVI je periodicky vysílána až do vypršení doby její přednastavené platnosti, nebo do doby, než příslušná RSU jednotka vyšle speciální IVI zprávu, která zruší platnost daných vysílaných dopravních informací. Specifikace IVI zprávy je detailně popsána v normě *ISO/TS 19321 Intelligent transport systems – Cooperative ITS – Dictionary of in-vehicle information (IVI) data structure*. Pro kódování jednotlivých dopravních symbolů bude primárně použita knihovna definována v normě *ISO/TS 14823 Traffic and travel information – Messages via media independent stationary dissemination systems – Graphic data dictionary for pre-trip and in-trip information dissemination systems*. Tento katalog zahrnuje běžné dopravní symboly, jejich číselný kód a doplňující informace. Struktura IVI zprávy je znázorněna na Obr. 6.



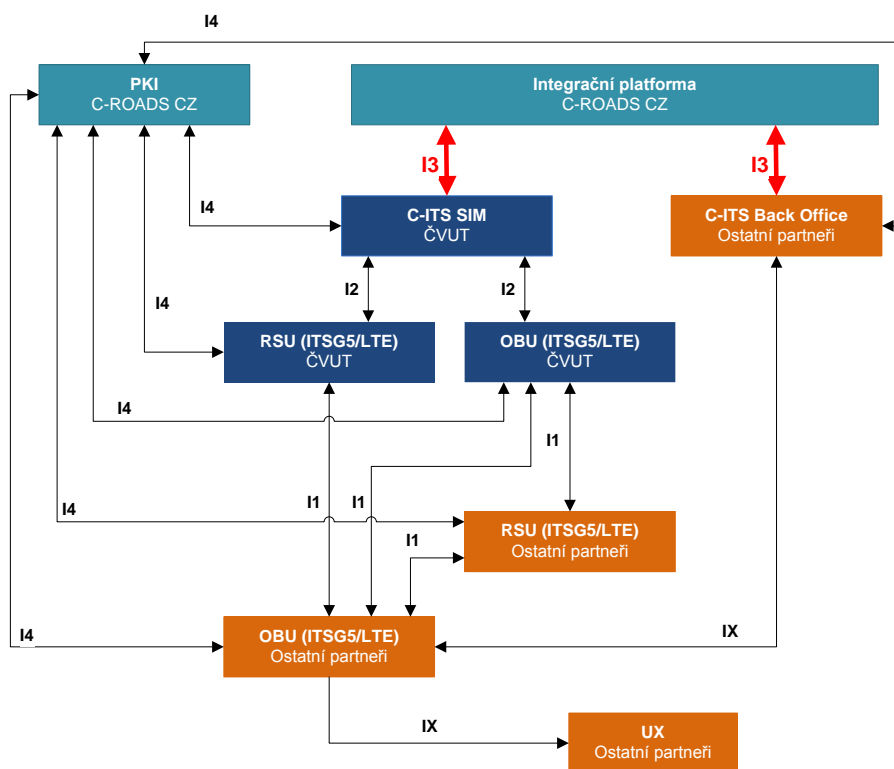
Obr. 6 Struktura zprávy IVI

- 5.4. **Signal Phase and Timing Message (SPAT).** Zprávy SPAT slouží k poskytování informací o signálním cyklu světelného signalizačního zařízení (SSZ) na křižovatkách. Tento cyklus určuje pořadí a délku jednotlivých signálních dob. SPAT je generována v jednotce RSU na základě informací z řadiče SSZ. Jedna tato zpráva může obsahovat informace o signálním cyklu jedné nebo více křižovatek zároveň. Po příjmu zprávy SPAT vozidlovou jednotkou OBU je tato zpráva zpracovávána dohromady se zprávou MAP (viz další typ zpráv), čímž je stanoven stav světelné signalizace pro každý segment komunikace (jednotlivé jízdní pruhy). Na základě těchto informací může OBU jednotka ve vozidle informovat řidiče o doporučené rychlosti, varovat před průjezdem křižovatky na signál „stůj“ nebo zajistit plynulý průjezd křižovatkou. Zprávy SPAT jsou standardizovány dokumentem *SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary* a *ISO/TS 19091 Intelligent transport systems — Co-operative ITS - Using V2I and I2V Communications for Applications Related to Signalized Intersections (SPAT, MAP with European extensions)*..
- 5.5. **Map Data (MAP).** Zprávy MAP slouží k poskytování informací o topologii a geometrii křižovatkových úseků z jednotek RSU do vozidel nebo do mobilních zařízení. Jedna zpráva MAP může obsahovat informace o geometrii jedné, ale i více křižovatek. Po příjmu zprávy MAP vozidlovou jednotkou OBU je tato zpráva zpracovávána dohromady se zprávou SPAT, čímž je stanoven stav světelné signalizace pro každý segment křižovatky (jednotlivé jízdní pruhy). Specifikace zprávy MAP je popsána v dokumentu *ISO/TS 19091 Intelligent transport systems — Co-operative ITS - Using V2I and I2V Communications for Applications Related to Signalized Intersections (SPAT, MAP with European extensions)*.
6. **Rozhraní I2: C-ITS SIM ↔ C-ITS jednotky.** Toto rozhraní bude řešeno několika nezávislými datovými streamy zajišťující různé funkční požadavky. Schéma na Obr. 7 zobrazuje architekturu umístění a napojení na rozhraní I2 pro budovaný C-ITS systém.



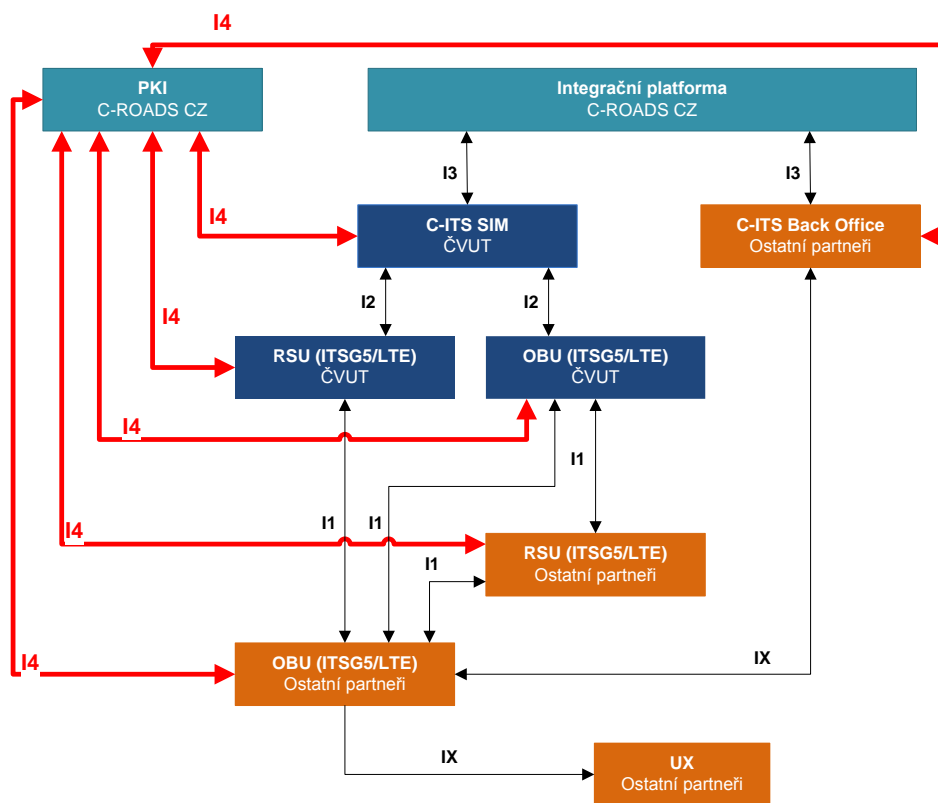
Obr. 7 Architektura umístění a napojení rozhraní I2

7. V rámci rozhraní I2 bude docházet k výměně těchto dat:
 - 7.1. Vlastní implementace UC pomocí C-ITS zprávy (CAM, DENM, IVI, SPAT-MAP). Tato komunikace bude probíhat oběma směry.
 - 7.2. Z C-ITS SIM na RSU/OBU jednotky budou zasílány požadavky na nastavení jednotek. Bude se jednat minimálně o tyto činnosti:
 - 7.2.1. Aktivace/deaktivace konkrétního RSU/OBU
 - 7.3. Aktivace/deaktivace konkrétního RSU/OBU
 - 7.4. Z RSU/OBU jednotek na C-ITS SIM budou pravidelně zasílány:
 - a) Stavové informace o RSU/OBU a jejich jednotlivých komponentách
8. Pro výměnu těchto dat mezi OBU/RSU a C-ITS SIM navrhne Dodavatel komunikační protokol. Na fyzické vrstvě bude toto rozhraní využívat pevné kabelové spojení a/nebo veřejnou mobilní síť LTE.
9. **Rozhraní I3: C-ITS back office ↔ Integrovaná platforma.** Toto rozhraní bude na straně C-ITS SIM připraveno na základě specifikací předaných Zadavatelem Dodavateli. Bude se jednat o specifikace připravené v rámci projektu C-ROADS Czech Republic. Přes toto rozhraní budou do C-ITS SIM předávány dopravní informace (zprávy DENM a IVI), které budou v C-ITS SIM dále analyzovány a vyhodnoceny. Naopak C-ITS zprávy přijaté z C-ITS jednotek a generované v C-ITS SIM budou přes toto rozhraní předávány dále do IP. Samotná integrace proběhne v průběhu realizace projektu. Dodavatel je povinen zajistit součinnost při této implementaci. Zadavatel zajistí, aby konsorcium C-ROADS Czech Republic poskytlo Dodavateli součinnosti při této implementaci. Schéma na Obr. 8 zobrazuje architekturu umístění a napojení na rozhraní I3 pro budovaný C-ITS systém.



Obr. 8 Architektura umístění a napojení rozhraní I3

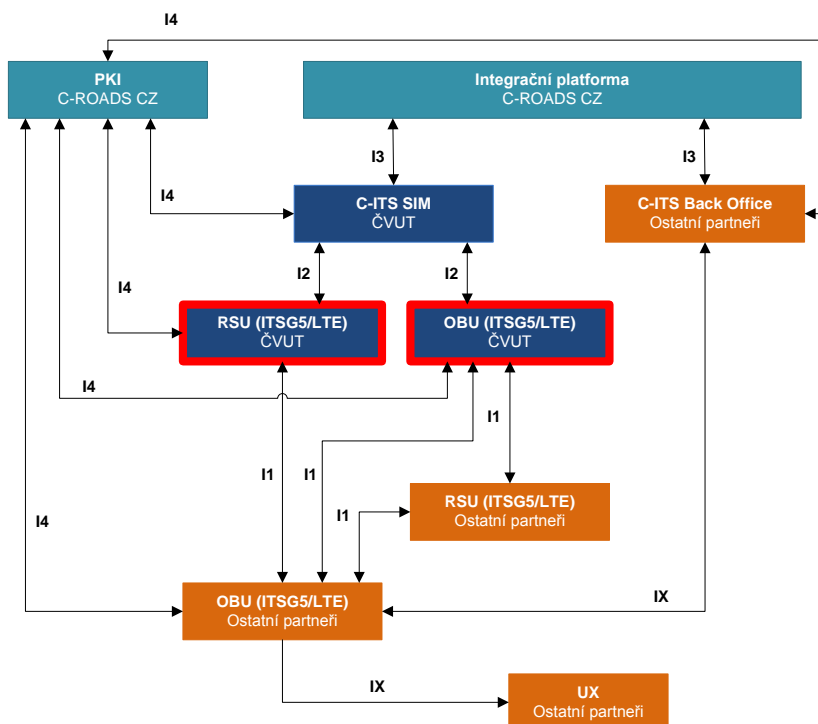
10. **Rozhraní I4: C-ITS SIM ↔ PKI infrastruktura.** Jedná se o rozhraní mezi Security částí C-ITS SIM a externím PKI infrastrukturou realizovanou konsorciem projektu C-ROADS Czech Republic (tj. Root CA, Enrolment CA, Authorization CA) pracující na technologii TeskaLabs SeaCat. V rámci tohoto rozhraní budou distribuovány mj. veřejné klíče C-ITS komponent, certifikáty a další data potřebná pro funkčnost PKI infrastruktury (např. CRL, CTL). Spojení s PKI infrastrukturou bude realizováno v součinnosti s konsorciem projektu C-ROADS Czech Republic formou instalace bezpečnostní brány (TeskaLabs SeaCat Gateway) do demilitarizované zóny C-ITS SIM. Veškerá komunikace a formáty certifikátů budou v souladu příslušnými normami (*ETSI TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, ETSI TS 102 941 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management v1.2.1, ETSI TS 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats v1.3.1*). Samotná integrace proběhne v rámci realizace této zakázky. Dodavatel je povinen zajistit součinnost při této implementaci. Zadavatel zajistí, aby členové konsorcia C-ROADS Czech Republic poskytli Dodavateli adekvátní součinnosti při této implementaci. Schéma na Obr. 9 zobrazuje architekturu umístění a napojení na rozhraní I4 pro budovaný C-ITS systém.



Obr. 9 Architektura umístění a napojení rozhraní I4

VIII. C-ITS JEDNOTKY

1. Součástí dodávky jsou také C-ITS jednotky umístěné ve vozidlech Zadavatele a slouží jako testovací vozidla pro ověření funkčnosti systému a jednotlivých služeb. V rámci tohoto projektu se jedná o RSU a OBU jednotky. Architektura umístění a napojení RSU/OBU jednotek v C-ITS systému budovaném v rámci projektu C-ROADS Czech Republic je uvedena na Obr. 10.



Obr. 10 Architektura umístění a napojení C-ITS jednotek (RSU a OBU)

2. Přímá datová konektivita do C-ITS SIM bude řešena buď přímým kabelovým připojením, nebo alternativně pomocí dedikované APN privátní sítě Zadavatele. SIM karty s pevnou IP adresou a dostatečným datovým tarifem (min. 10 Gb/měsíc na jednu SIM) budou poskytnuty Zadavatelem Dodavatel. V rámci tohoto projektu budou vybavena 2 vozidla Zadavatele RSU/OBU jednotkou. Tyto jednotky vč. anténního systému a napájení musí být možné demontovat a umístit je v laboratořích pro interní testování ve specifických podmínkách.
3. K zobrazení informací řidiči ve vozidle, popř. možnosti manuálního zadání dat do systému, bude sloužit přímé kabelové spojení s C-ITS SIM.
4. Parametry ITS-G5 zpráv (DENM, CAM) mohou být určovány na základě dat z GNSS přijímače (poloha, rychlost, zrychlení aj.) či aplikační logiky uvnitř OBU. Jednotka OBU musí obsahovat SW vrstvy v souladu se standardem ETSI (ITS Access Technology Layer, ITS Network & Transport Layer, ITS Facility Layer, ITS Application Layer), přičemž aplikační vrstva musí obsahovat aplikace definované pro výše popsané C-ITS služby. K této aplikační logice budou dodány v rámci realizace této veřejné zakázky příslušné SW licence.
5. **Funkční požadavky na RVU/OBU jednotky.** Dodávané jednotky musí splňovat následující funkční požadavky:
 - 5.1. Požadavky na provoz RSU/OBU:
 - a) jednotka RSU/OBU je klientem a C-ITS SIM je serverem;
 - b) RSU/OBU musí být schopna detekovat přerušené spojení mezi jednotkou a C-ITS SIM;
 - c) v případě přerušení spojení mezi jednotkou a C-ITS SIM se iniciátor (RSU/OBU) pokusí znovu navázat spojení;
 - d) RSU/OBU musí zaznamenávat údaje o přerušovaných spojeních a vyřazených datech;

- e) RSU/OBU jednotka musí umožňovat implementaci Public Key Infrastructure (PKI) mechanismů – správa certifikátů a klíčů pro komunikaci a návazné kryptografické procesy;
- f) RSU/OBU jednotka musí umožňovat detekci poruchových stavů (autodiagnostika).

5.2. Požadavky na nastavení jednotky RSU/OBU:

- a) čas na všech jednotkách RSU/OBU musí být synchronizován vůči společnému referenčnímu času poskytnutému z C-ITS SIM (NTP) nebo z GNSS signálu;
- b) všechny jednotky RSU/OBU musí být vzdáleně konfigurovatelné z C-ITS SIM;
- c) RSU/OBU jednotky musí umožnit update firmwaru a SW stacku;
- d) RSU/OBU jednotka musí být schopna aktivace tzv. koexistenčního módu;
- e) RSU/OBU jednotka musí umožňovat uložení minimálně 16 poloh mýtných bran do paměti jednotky pro účely tzv. koexistenčního módu.

5.3. Požadavky na rozhraní jednotky RSU/OBU:

- a) jednotka RSU/OBU musí komunikovat s jednotkami OBU/RSU třetích stran pomocí ITS-G5 komunikace definované v předpisu *ETSI EN 302 663 Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band*;
- b) jednotka RSU/OBU musí být schopna zašifrovat/dešifrovat C-ITS zprávy pomocí protokolu Geo Network (GN) definovaného v předpisech *ETSI EN 302 636 1, 2, 3, 4, 6 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking*;
- c) Jednotka RSU/OBU musí být schopna zašifrovat/dešifrovat C-ITS zprávy pomocí protokolu Basic Transport Protocol (BTP) definovaného v předpisu *ETSI EN 302 636 5 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking*;
- d) jednotka RSU/OBU musí komunikovat s C-ITS SIM prostřednictvím pevného kabelového spojení nebo veřejných sítí mobilních operátorů;
- e) Podoba komunikačních rozhraní na další prvky C-ITS systému je popsána v rámci článku VII.

5.4. Požadavky na zpracování dat RSU/OBU:

- a) Zprávy CAM:
 - jednotka RSU/OBU musí být schopna šifrovat/dešifrovat, podepisovat/ověřovat podpis a přijímat/odesílat CAM pakety z/do jednotek OBU/RSU;
 - jednotka RSU/OBU musí být schopna na základě CAM zprávy z RSU aktivovat koexistenční mód v ochranných zónách mýtných bran (viz článek XI).
- b) Zprávy DENM
 - jednotka RSU/OBU musí být schopna šifrovat/dešifrovat, podepisovat/ověřovat podpis a odesílat/přijímat DENM pakety pomocí protokolu Geo Broadcast Mode z/do jednotek OBU/RSU definovaném v předpisu *ETSI 103 301 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services*;
 - jednotka RSU/OBU musí být schopna přijímat DENM zprávy z C-ITS SIM a vysílat je prostřednictvím ITS-G5;

- jednotka RSU/OBU musí být schopna vytvořit DENM zprávy na základě manuálního vytvoření události v C-ITS SIM a vysílat je prostřednictvím ITS-G5;
- jednotka RSU/OBU musí být schopna vytvořit DENM zprávu varující o průjezdu na červenou (use case ISV) na základě vyhodnocení přijatých SPAT a MAP zpráv a informací o vlastní rychlosti a zrychlení.
- c) Zprávy IVI:
 - jednotka OBU musí být schopna dešifrovat a ověřovat podpis zprávy IVI;
 - jednotka OBU musí být schopna přijmout zprávy IVI z RSU.
- d) Zprávy SPAT
 - jednotka OBU musí být schopna dešifrovat a ověřovat podpis zprávy SPAT a vyhodnotit jejich obsah.
- e) Zprávy MAP
 - jednotka OBU musí být schopna dešifrovat a ověřovat podpis zprávy MAP a vyhodnotit jejich obsah.
- f) SSM / SRM
 - jednotka OBU musí být schopna vyslat a přijmout SSM a SRM zprávu z RSU jednotky a vyhodnotit jejich obsah.

6. **Technické požadavky na RVU/OBU jednotky.** Dodávané jednotky musí splňovat následující technické požadavky.

6.1. Provozní technické požadavky:

- a) modul pro rádiovou komunikaci ITS-G5 (5855 MHz až 5925 MHz) umožňující souběžnou komunikaci na dvou kanálech („Dual concurrent channel operation“);
- b) všesměrový anténní systém pracující v pásmu 5,9 GHz (ITS-G5) o minimálním zisku pro jeden vysílací kanál 5dBi splňující standard *ETSI 302 571 Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive*. Přesné umístění anténního systému na vozidle bude podléhat schválení Zadavatele;
- c) komunikační LTE modul včetně antény pro zajištění komunikace s C-ITS SIM prostřednictvím sítě mobilních operátorů (sekundární komunikační rozhraní s C-ITS SIM);
- d) komunikační rozhraní ETHERNET nebo obdobné (primární komunikační rozhraní s C-ITS SIM);
- e) GNSS přijímač pro určení přesné polohy a času vč. antény;
- f) další I/O vstupy (min. rozhraní RS232 nebo USB nebo GPIOs);
- g) dostatečná úroveň krytí odpovídající umístění zařízení (např. IP65 v případě umístění zařízení mimo interiér vozidla);
- h) provozní teplota min. v rozsahu -30°C až +65°C pro jednotky umístěné mimo interiér vozidel;
- i) napájení 12 – 24 V DC;
- j) vhodné datové úložiště, min. 4 GB (např. µSD paměťová karta);
- k) LED indikující stav zařízení;
- l) Hardware Security Module (HSM) - kompatibilní s TPM 1.2 (podporující TLS 1.2) a PKCS #11, splňující Common Criteria Certificate EAL4+;
- m) licence softwarového řešení pro RSU/OBU jednotky, tj. ITS software stack pro provoz C-ITS aplikací vč. přenosu C-ITS zpráv a SW aplikace umožňující

nasazení logiky zpracování C-ITS zpráv a vzdálenou správu ITS jednotek dle této ZD;

- n) prostorová data pro automatické vytvoření atributu Traces – prostorová data Zadavatel nespecifikuje;
- o) instalace RSU/OBU jednotek nesmí omezit či ovlivňovat stávající funkčnost jiných zařízení ve vozidlech ani vozidel samotných;
- p) RSU/OBU jednotky musí být lehce demontovatelné a přenositelné pro účely interních laboratorních testování.

6.2. **Bezpečnostní technické požadavky:** Ve vazbě na implementaci PKI infrastruktury musí jednotky splňovat určité požadavky. Tyto požadavky vycházejí z nutnosti instalace prvku PKI infrastruktury (SeaCat Client) do RSU/OBU jednotky. Jedná se o SW knihovnu zajišťující potřebné operace pro správnou funkčnost PKI systému (distribuce klíčů, aktualizace TLM, CRL apod.). Pro integraci tohoto prvku jsou na RSU/OBU kladeny následující požadavky:

- a) Operační systém – podpora jednoho z následujících:
 - Android 5.0+
 - Linux
 - Windows 8.1+
 - FreeBSD
- b) Klient PKI bude samostatný proces na úrovni operačního systému nebo C knihovna integrovaná přímo do aplikace RSU/OBU.
- c) Minimální požadavky na podporovaný HW:
 - CPU (1 jádro) – jedno z následujících:
 - x86 (32bit)
 - x86-64 (64bit)
 - ARM v6, v7, v8 s MMU
 - MIPS (32bit a 64bit)
 - Paměťová náročnost
 - 200 kb
 - Diskový prostor
 - 2 MB
 - Síťové rozhraní
 - IPv4 anebo IPv6 přes Ethernet, GSM/LTE
 - Sériová linka (e.g. RS-232) nebo USB

6.3. **Umístění RSU/OBU jednotek.** RSU/OBU jednotka bude umístěna ve vozidle tak, aby co nejméně omezovala jeho běžný provoz. Jednotka bude napájena z el. sítě vozidla. Způsob napojení na napájení nesmí narušit provoz vozidel a jejich případnou záruku, doporučuje se využít volný 12 V „autozapalovač“. Anténní systém jednotky pro příjem GPS, 4G a ITS-G5 bude instalován na vhodném místě, tak aby byl zajištěn dostatečný příjem signálu (GPS, GSM), a zároveň aby byl zajištěn dostatečný dosah signálu ITS-G5. Zadavatel umožňuje využití magnetických (nebo obdobných) upevňovacích prvků. Dodavatel je povinen před vlastní instalací anténního systému požádat Zadavatele o schválení konkrétního umístění.

IX. POŽADAVKY NA MOBILNÍ PRACOVNÍ STANICI

1. Požadavky na dodávanou mobilní pracovní stanici jsou následující:
 - 1.1. procesor min. INTEL Core i5 se 4 jádry nebo srovnatelný;
 - 1.2. operační paměť 16 GB RAM;
 - 1.3. HSM modul kompatibilní s TPM 1.2 (podporující TLS 1.2) a PKCS #11, splňující Common Criteria Certificate EAL4+ a FIPS 140-2 Level 3+;
 - 1.4. podpora minimálně následujících kryptografických algoritmů ECC pro digitální podepisování C-ITS zpráv v rozsahu:
 - a) ECDSA_nistP256_with_SHA256;
 - b) ECDSA_brainpoolP256r1_with_SHA256;
 - c) ECDSA_brainpoolP385r1_with_SHA384;
 - 1.5. Pevný disk min. 2 TB s rychlostí min. 7 000 ot./min.;
 - 1.6. Operační systém Windows 10 nebo Linux;
 - 1.7. Velikost displeje min. 15,6“.
2. Základní technické podmínky realizace C-ITS SIM jsou představovány platformou operačního systému, platformou databázového systému, jazykovou lokalizací a požadavky na typ informačního systému. V tomto smyslu budou:
 - 2.1. C-ITS SIM bude pracovat na platformě plně kompatibilní s Microsoft Windows nebo Linux;
 - 2.2. všechny interní databáze C-ITS SIM budou pracovat nad jedním databázovým produktem;
 - 2.3. součásti vnitřní logiky systému C-ITS SIM budou pracovat na principech geografických informačních systémů;
 - 2.4. geografická lokalizace bude v rámci C-ITS SIM probíhat ve vztahu k dodanému mapovému podkladu; předpokládá se použití Open Street Map (OSM);
 - 2.5. komponenty všech částí uživatelského rozhraní budou lokalizovány v českém jazyce.

X. POŽADAVKY NA BEZPEČNOST C-ITS SYSTÉMU

1. **Základní požadavky na systémovou bezpečnost.** Dodávaný systém musí splňovat následující vlastnosti, které zajistí, že:
 - 1.1. systémem uchovávaná data nebudou zpřístupněna neautorizovaným osobám; přístup a veškerá manipulace s daty musí být zaznamenávána do provozních logů.
 - 1.2. data budou během komunikace chráněna proti zneužití neautorizovanou osobou;
 - 1.3. systémem uchovávaná data nebude možné změnit nebo poškodit neautorizovanou osobou, či administrátory správce nebo provozovatele;
 - 1.4. kryptografický materiál bude chráněn proti kompromitaci a zneužití (tj. implementace HSM nebo možnost využití SW implementace HSM na mobilním PC pro Admin uživatele).

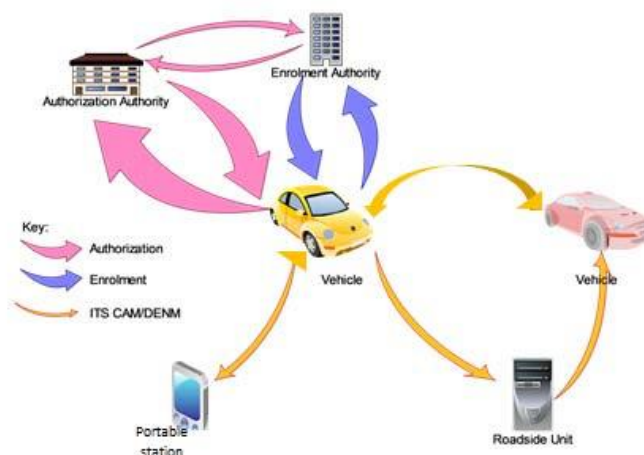
2. Bezpečnostní otázky se definují v rámci strategického dokumentu: „COM (2016) 766 - A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility“.
3. **Podporované kryptografické standardy.** Standardy řešení projektu C-ROADS Czech Republic vyžadují u všem klíčových komponent implementaci bezpečnostních postupů a standardů rodiny Public Key Infrastructure (PKI), využívající správu a distribuci veřejných klíčů asymetrickou kryptografií. Využití této technologie vychází ze současného trendu v oblasti kooperativních systémů C-ITS, a to zejména z důvodu jednoduché distribuce veřejných klíčů. Dodávané C-ITS jednotky proto musí podporovat minimálně následující kryptografické algoritmy:
 - 3.1. ECDSA_nistP256_with_SHA256
 - 3.2. ECDSA_brainpoolP256r1_with_SHA256
 - 3.3. ECDSA_brainpoolP384r1_with_SHA384
4. **Bezpečnostní funkce.** Bezpečnostní řešení dodávaného C-ITS systému musí mít implementované minimálně následujících funkcionalit:
 - 4.1. Vygenerování páru asymetrických klíčů
 - 4.2. Vydání nového certifikátu
 - 4.3. Obnova expirovaného / revokovaného certifikátu
 - 4.4. Přihlášení nového zařízení do sítě
 - 4.5. Podpis datové zprávy DENM
 - 4.6. Kontrola přijaté podepsané datové zprávy DENM
 - 4.7. Správa certifikátů
 - 4.8. Revokace certifikátů
5. **Zajištění interoperability systému.** Hlavní požadavky na interoperabilitu bezpečnostního řešení v rámci celého projektu C-ROADS Czech Republic vycházejí z dodržování schválených dokumentů a norem, které jsou uvedeny v následující tabulce.

Oblast	Definiční dokument / norma
Governance	C-ITS Security Policy & Governance Framework Release 1
Trust Model	C-ITS Certificate Policy Release 1
Certificate Data Structure	ETSI TS 103 097 v.1.3.1
Cryptographic Algorithms	ETSI TS 103 097 v.1.3.1 (ECDSA, NIST and Brainpool) C-ITS Certificate Policy v1.0
Download C-ROADS CTL	ETSI TS 102 941 (1.2.1)
Download C-ROADS CRL	ETSI TS 102 941 (1.2.1)
C-ROADS CTL data structure	ETSI TS 102 941 (1.2.1)
C-ROADS CRL data structure	ETSI TS 102 941 (1.2.1) ETSI TS 102 941 (1.2.1)

Verification Algorithm for Certificate/ Signature	Only for ETSI TS 103 097 v.1.2.1
--	----------------------------------

6. **Aktéři bezpečnostního řešení C-ROADS Czech Republic.** V této kapitole jsou popsáni nezbytní aktéři, kteří se budou na zajišťování bezpečnosti přenášených C-ITS zpráv pro projekt C-ROADS Czech Republic podílet, struktura jejich vzájemných interakcí je uvedena na Obr. 11. Jedná se o následující aktéry:

- 6.1. Národní certifikační autorita
 - a) Root CA
 - b) Enrolment authority (dle ETSI TS 102 940)
 - c) Authorization authority (dle ETSI TS 102 940)
- 6.2. Jednotka na infrastruktuře (RSU)
- 6.3. Mobilní jednotka (OBU)
- 6.4. C-ITS SIM (nebo C-ITS Back Office)
- 6.5. Mobilní zařízení / aplikace
- 6.6. Uživatel

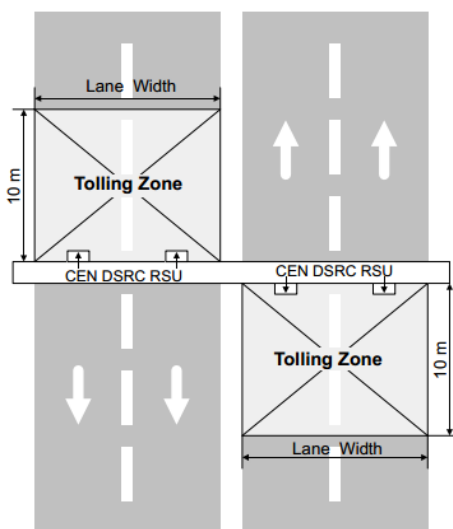


Obr. 11 Schéma aktérů systému C-ROADS dle ETSI 102 940

XI. KOEXISTENCE SE STÁVAJÍCÍMI SYSTÉMY DSRC

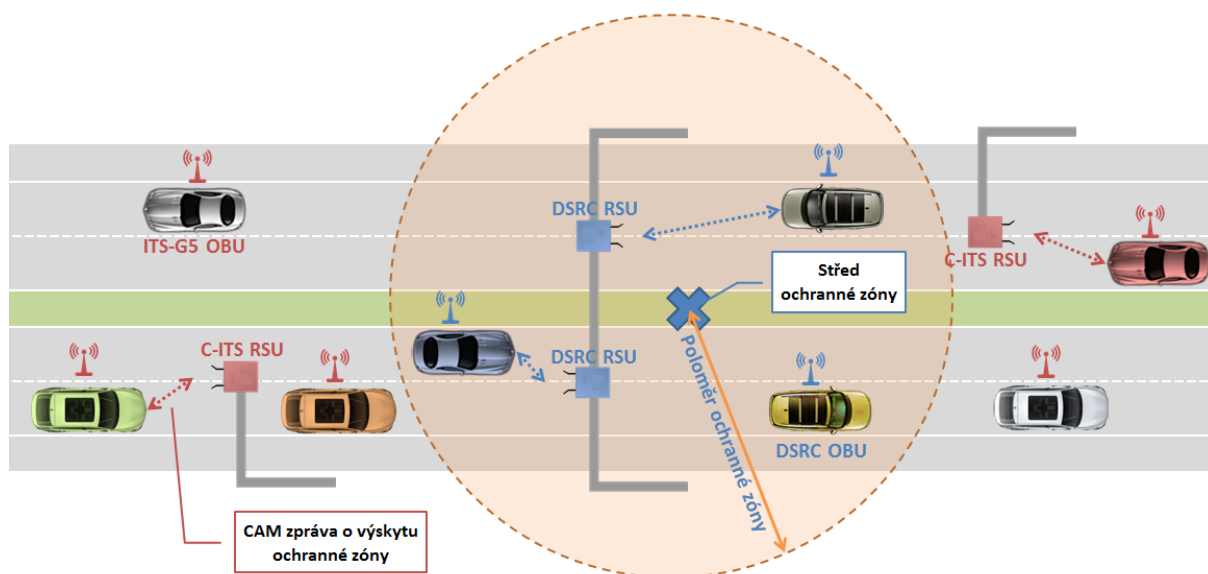
1. Tato kapitola poskytuje přehled informací o koexistenci technologie ITS-G5 a stávající technologie CEN-DSRC využívané pro výběr elektronického mýta na dálnicích a silnicích I. třídy. Kooperativní systém na bázi technologie ITS-G5 zajišťující komunikaci mezi vozidly a infrastrukturou (V2V a V2I) využívá vyhrazené frekvenční pásmo 5,9 GHz. V sousedním frekvenčním pásmu 5,8 GHz pracuje již zavedený systém výběru elektronického mýta pomocí technologie CEN-DSRC, umístěné zpravidla na mýtných portálech. Právě díky blízkému sousedství obou frekvenčních pásem (ochranné pásmo 20 MHz) může potenciálně dojít k nežádoucímu rušení signálu.

2. Zavádění technik zmírnění vlivu technologie ITS-G5 na provoz mýtných systémů je povinný a tyto techniky jsou popsány v normách *ETSI TS 102 792 Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range* a *ETSI EN 302 571 Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive*. Dodávané řešení proto musí splňovat pravidla stanovené v těchto normách.



Obr. 12 Příklad zóny výběru mýta pomocí CEN-DSRC dle ETSI 102 792

3. Pro zmírnění potenciální radiové interference mezi frekvenčními pásmy 5,8 GHz a 5,9 GHz byly identifikovány dvě hlavní cesty:
- 3.1. Omezení vyzářeného výkonu ITS-G5:
 - a) ve vyhrazeném frekvenčním pásmu;
 - b) mimo vyhrazené frekvenční pásmo.
 - 3.2. Omezení času, kdy ITS-G5 jednotka vysílá:
 - a) přenosový čas T_{on} – C-ITS jednotka může vysílat pouze v tento časový interval;
 - b) doba nečinnosti T_{off} – C-ITS jednotka v tomto časovém intervalu nevysílá žádné zprávy.
4. V blízkosti mýtných portálů s technologií CEN-DSRC 5,8 GHz, které komunikují s mobilními jednotkami pro výběr elektronického mýta umístěnými ve vozidle, C-ITS jednotky budou fungovat pouze v „koexistenčním módu“, který využívá jednu nebo obě cesty ke zmírnění rušení signálu uvedené v textu výše. Druhy koexistenčních módů a jejich kombinace limitů vysílacího výkonu a omezení střídy jsou uvedeny v *ETSI 102 792 Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range*. Mimo tyto zóny není nutné aplikovat žádné koexistenční módy.



Obr. 13 Příklad koexistence mezi ITS-G5 a CEN-DSRC

5. **Detekce ochranných zón.** Vozidlové jednotky C-ITS technologie (OBU) budou schopny detekovat, zda se nacházejí v ochranném pásmu a v případě potřeby budou aktivovat jeden z koexistenčních módů. Informace o ochranných zónách v případě mýtných portálů obsahuje následující položky:
 - 5.1. střed ochranné zóny;
 - 5.2. poloměr ochranné zóny.
6. V rámci pilotního ověřování ITS-G5 technologií bude zajištěna koexistence ITS-G5 technologie s technologií CEN-DSRC mýtných portálů rozesláním upozornění na polohu ochranných zón mýtných portálů prostřednictvím CAM zpráv, přičemž zdrojem vysílání těchto zpráv budou C-ITS RSU jednotky na dotčených komunikacích nebo C-ITS SIM, který bude informovat OBU jednotku o výskytu DSRC mýtné brány. Jedna RSU jednotka bude vždy vysílat informace pouze o několika následujících ochranných zónách (maximálně 16 zón). Informace o poloze mýtných bran budou do jednotlivých RSU jednotek jednorázově nastaveny ještě před instalací na lokality.
7. Parametry pro přenos informací o ochranných zónách. Struktura zprávy CAM je detailně popsána v normě *ETSI EN 302 637 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications*; a jednotlivé atributy CAM zprávy jsou podrobně popsány v normě *ETSI TS 102 894-2 Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary*. Atributy datového kontejneru, který se stará o přenos informací o ochranné zóně prostřednictvím CAM zpráv, jsou uvedeny v tabulce níže.

RSU Container High Frequency	
protectedZoneType	Typ ochranné zóny – cenDsrcTolling (0)
expiryTime TimestampIts	Doba platnosti informace o dané ochranné zóně

protectedZoneLatitude	Zeměpisná šířka středu ochranné zóny
protectedZoneLongitude	Zeměpisná délka středu ochranné zóny
protectedZoneRadius	Poloměr ochranné zóny [m]
protectedZoneID	Id ochranné zóny

Tabulka 1 Atributy pro přenos informace o ochranné zóně ve zprávě CAM

XII. POŽADAVKY NA DOKUMENTACI

1. Veškerá dokumentace musí být Zadavateli předána v tištěné i elektronické podobě (ve formátu DOC nebo DOCX) v českém jazyce. Dokumentace musí být zpracovaná v míře podrobnosti umožňující následující provoz a správu systému bez přímého zapojení původního Dodavatele systému.
2. Dokumentace skutečného provedení bude připravena minimálně v následujícím rozsahu:
 - 2.1. Technická zpráva (vč. popisu funkcionality, jednotlivých rozhraní a protokolů), tj. popis skutečného provedení systému a veškerých komponent;
 - 2.2. Soupis hlavních komponent zařízení;
 - 2.3. Certifikáty k dodanému HW včetně prohlášení o shodě (případně další dokumentace, standardně dodávaná výrobcem);
 - 2.4. Uživatelské návody a příručky:
 - a) Uživatelská příručka:
 - Postup práce s dodaným systémem;
 - Organizačně provozní zajištění dodaného systému;
 - Řešení nestandardních stavů systému, scénáře řešení;
 - Aplikační nápověda.
 - b) Instalační příručka:
 - Instalace a konfigurace C-ITS komponent.
 - c) Školící materiály pro administrátory systému.
 - d) Návody a postupy k dodanému HW.

XIII. SOUVISEJÍCÍ PŘEDPISY A NORMY

1. Při řešení projektu musí být Dodavatelem respektovány vyhlášky, předpisy a normy platné v době zpracování projektu, včetně norem souvisejících v aktuálním znění a technických podmínek výrobce, zejména pak:
 - 1.1. ČSN 33 2130 ed. 2 (Elektrické instalace nízkého napětí - Vnitřní elektrické rozvody z 9.2009),
 - 1.2. ČSN 34 2300 (Předpisy pro vnitřní rozvody sdělovacích vedení),

- 1.3. ČSN 33 2000-1 ed. 2 (Elektrické instalace nízkého napětí - Část 1: Základní hlediska, stanovení základních charakteristik, definice z 5.2009),
- 1.4. ČSN 33 2000-4-41 ed. 2 (Elektrické instalace nízkého napětí - Část 4-41: Ochranná opatření pro zajištění bezpečnosti - Ochrana před úrazem elektrickým proudem z 8.2007 a změny Z1 z 4.2010),
- 1.5. Podle ČSN 33 2000-5-51 ed. 3 (Elektrické instalace nízkého napětí - Část 5-51: Výběr a stavba elektrických zařízení - Všeobecné předpisy z 4.2010),
- 1.6. ČSN 33 2000-5-52 ed.2 (Elektrotechnické předpisy - Elektrická zařízení - Část 5: Výběr a stavba elektrických zařízení – Část 5-52: Elektrická vedení z 12.2012),
- 1.7. ČSN 33 2000-5-54 ed. 2 (Elektrické instalace nízkého napětí - Část 5-54: Výběr a stavba elektrických zařízení - Uzemnění, ochranné vodiče a vodiče ochranného pospojování z 9.2007),
- 1.8. ČSN 33 2000-6 (Elektrické instalace nízkého napětí - Část 6: Revize z 9.2007),
- 1.9. Řada norem ČSN EN 62305 (Ochrana před bleskem z 7.2007),
- 1.10. ČSN EN 60664-1 ed. 2 (Koordinace izolace zařízení nízkého napětí - Část 1: Zásady, požadavky a zkoušky z 4.2008),
- 1.11. ČSN EN 61000-4-30 ed. 2 (Elektromagnetická kompatibilita (EMC) - Část 4-30: Zkušební a měřicí technika - Metody měření kvality energie z 9.2009),
- 1.12. ČSN EN 61000-4-6 ed. 3 (Elektromagnetická kompatibilita (EMC) - Část 4-6: Zkušební a měřicí technika - Odolnost proti rušením šířeným vedením, indukovaným vysokofrekvenčními poli z 11.2009),
- 1.13. ČSN EN 61140-4-6 ed. 2 (Ochrana před úrazem elektrickým proudem - Společná hlediska pro instalaci a zařízení z 3.2003),
- 1.14. ČSN 33 4000 (Elektrotechnické předpisy. Požadavky na odolnost sdělovacích zařízení proti přepětí a nadproudu z 8.1988),
- 1.15. ČSN 33 4010 (Elektrotechnické předpisy. Ochrana sdělovacích vedení a zařízení proti přepětí a nadproudu atmosférického původu z 11.1990),
- 1.16. ČSN EN 60079-14 ed. 3 (Výbušné atmosféry - Část 14: Návrh, výběr a zřizování elektrických instalací z 4.2009),
- 1.17. ČSN 73 6005 (Prostorové uspořádání sítí technického vybavení)
- 1.18. ČSN 73 6006 (Výstražné fólie k identifikaci podzemních vedení technického vybavení)
- 1.19. řada norem ČSN EN 50173-x (Informační technologie – Univerzální kabelážní systémy),
- 1.20. řada norem ČSN EN 50174-x (Informační technologie – Instalace kabelových rozvodů),
- 1.21. řada norem ČSN 73 08xx (Požární bezpečnost staveb),
- 1.22. MP 400 (Zabezpečení objektů pozemních komunikací před odcizením nebo úmyslným poškozením – Část 400 Elektro a sdělovací objekty. Metodický pokyn Odboru pozemních komunikací a územního plánu Ministerstva dopravy)

- 1.23. CEN TS 16157-1 Inteligentní dopravní systémy – Specifikace výměnného formátu DATEX II pro řízení dopravy a dopravní informace – Část 1: Obecný rámec a architektura
- 1.24. CEN TS 16157-2 Inteligentní dopravní systémy – Specifikace výměnného formátu DATEX II pro řízení dopravy a dopravní informace – Část 2: Označování pozice
- 1.25. EN TS 16157-3 Inteligentní dopravní systémy – Specifikace výměnného formátu DATEX II pro řízení dopravy a dopravní informace – Část 3: Publikace situace
- 1.26. TP 66 (Zásady pro označování pracovních míst na pozemních komunikacích)
- 1.27. TP 141 (Zásady pro systémy proměnného dopravního značení a zařízení pro proměnné provozní informace na pozemních komunikacích)
- 1.28. TP 172 (Dopravní informační centra)
- 1.29. TP 182 (Dopravní telematika na pozemních komunikacích)
2. Navržené řešení musí být v souladu s platnými evropskými i světovými standardy a směrnicemi pro použití C-ITS a přenosových protokolů. Bude se jednat zejména o tyto předpisy:
 - 2.1. ETSI 101 539-1 Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification
 - 2.2. ETSI 102 637-1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements
 - 2.3. ETSI 102 638 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions
 - 2.4. ETSI 102 894-2 Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary
 - 2.5. ETSI 103 301 Intelligent Transport Systems (ITS) - Vehicular Communications – Basic Set of Applications – Facilities layer protocols and communication requirements for I2V messages
 - 2.6. ETSI 302 637-2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
 - 2.7. ETSI 302 637-3 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
 - 2.8. ETSI 102 687 Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part
 - 2.9. ETSI 102 724 Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band
 - 2.10. ETSI 102 731 Intelligent Transport Systems (ITS); Security; Security Services and Architecture
 - 2.11. ETSI TS 102 792 Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN

- DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range
- 2.12. ETSI 102 894-1 Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications
 - 2.13. ETSI 102 894-2 Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary
 - 2.14. ETSI 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats
 - 2.15. ETSI 103 301 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services
 - 2.16. ETSI 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
 - 2.17. ETSI 102 941 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
 - 2.18. ETSI 102 942 Intelligent Transport Systems (ITS); Security; Access Control
 - 2.19. ETSI 302 636-4-1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality
 - 2.20. ETSI EN 302 637 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications;
 - 2.21. ETSI 302 663 Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
 - 2.22. ETSI 302 665 Intelligent Transport Systems (ITS); Communications Architecture
 - 2.23. ETSI 302 571 Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
 - 2.24. ETSI 302 931 Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition
 - 2.25. ETSI 202 663 Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band
 - 2.26. ISO 19321 Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures
 - 2.27. ISO 19091 Intelligent transport systems - Co-operative ITS - Using V2I and I2V Communications for Applications Related to Signalized Intersections (SPAT, MAP with European extensions)
 - 2.28. ISO 14823 Traffic and travel information - Messages via media independent stationary dissemination systems - Graphic data dictionary for pre-trip and in-trip information dissemination systems

- 2.29. ISO 17425 Intelligent transport systems - Cooperative systems - Data exchange specification for in-vehicle presentation of external road and traffic related data
- 2.30. ISO 29281 Intelligent transport systems - Communication access for land mobiles (CALM) - Non-IP networking
- 2.31. ISO 21215 Intelligent transport systems - Communications access for land mobiles (CALM) - M5
- 2.32. IEEE Std 802.11p IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment 6: Wireless Access in Vehicular Environments
- 2.33. RFC 6275 Mobility Support in IPv6
- 2.34. IETF RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

XIV. VŠEOBECNÁ ČÁST

1. Dodavatel dodá C-ITS systém dle této technické specifikace. Vlastní dodávka bude realizována v etapách uvedených v čl. IV odst. 1 Smlouvy o dodávce hardware a software a poskytnutí souvisejících služeb:
2. **Průběh a ukončení Etapy T1.** Etapa T1 této dodávky bude ukončena tím, že Dodavatel předá Zadavateli systém C-ITS dle této Technické specifikace. O předání sepíše Dodavatel a Zadavatel Předávací protokol. Vedle případných dalších bodů uvedených ve Smlouvě o dodávce hardware a software a poskytnutí souvisejících služeb je podepsání Předávacího protokolu podmíněno splněním i následujících bodů:
 - 2.1. Dokončení a splnění všech částí Etapy T1 dodávky;
 - 2.2. Předání dokumentace uvedeném v článku XII;
 - 2.3. Předání příslušných zkušebních protokolů z individuálních zkoušek, které jsou popsány dále v tomto článku, a to minimálně následujících komponent systému:
 - a) C-ITS jednotky ve formě RSU a OBU včetně souvisejícího příslušenství;
 - b) C-ITS SIM ve formě instalovaného SW na dodaném mobilním PC
3. Dnem podpisu Předávacího protokolu vyzývá Dodavatel Zadavatele ke společnému testování, a dodávka tak vstupuje do Etapy T2.
4. **Individuální zkoušky.** Součástí Etapy T1 bude provedení individuálních zkoušek. Tyto zkoušky provede Dodavatel a v rámci předání C-ITS systému Zadavateli předloží dokumentaci o provedení těchto zkoušek. Individuální zkoušky se budou skládat z několika částí. Tyto části jsou popsány podrobněji v textu níže. Výstupem individuálních zkoušek bude povinná dokumentace k C-ITS jednotkám a záznamové archy s výsledky funkčních zkoušek. Pro splnění individuálních zkoušek je potřeba splnit všechny části testování.
 - 4.1. **Certifikace komponentů.** Podmínkou splnění individuálních zkoušek je doložení povinné dokumentace daného výrobce C-ITS jednotek (např. dokument „ES prohlášení o shodě“, popřípadě výčet příslušných norem, které dané zařízení splňuje potvrzené výrobcem zařízení). Tyto dokumenty dokládají, že výrobce zařízení správně posoudil

shodu výrobku s požadavky příslušných norem a nařízeními vlády. V rámci této části individuálních zkoušek budou také k dodávaným C-ITS jednotkám doložen alespoň 1 certifikát nebo prohlášení organizátora testů o úspěšném provedení testů pro zajištění mezinárodní interoperability.

- 4.2. **Funkční zkoušky.** V této části budou testovány funkce konkrétních jednotek, které jsou definovány níže. Podkladem pro provedení funkčních zkoušek budou testovací scénáře, které vypracuje Dodavatel na základě podkladů poskytnutých Zadavatelem. Dodavatel následně tyto testovací scénáře před započítím zkoušek předloží Zadavateli ke schválení. Při těchto testech bude prověřována schopnost jednotek OBU/RSU generovat a přijímat standardizované ITS-G5 zprávy. V rámci této úrovně zkoušek budou testovány minimálně následující funkce C-ITS systému:
- a) Jednotky RSU
 - Příjem ITS-G5 zpráv (min. CAM) od projíždějících vozidel
 - Generování ITS-G5 zpráv (CAM, DENM, IVI, SPAT, MAP)
 - b) Jednotky OBU
 - Příjem ITS-G5 zpráv (min. CAM, DENM) od projíždějících vozidel nebo blízkých RSU
 - Generování ITS-G5 zpráv (min. CAM, DENM)
- 4.3. Výstupy funkčních zkoušek jednotlivých zařízení budou zaznamenány do záznamového archu, který bude obsahovat min. následující informace:
- a) Název zařízení
 - b) Umístění zařízení
 - c) Heat mapa
 - d) Název testované funkce
 - e) Výsledek
 - f) Datum zkoušek
 - g) Jméno testera
 - h) Podpis testera
- 4.4. **Komplexní zkoušky.** Komplexní zkoušky budou společně provádět zástupci Dodavatele, Zadavatele a vybraní partneři projektu C-ROADS Czech Republic. V rámci komplexních zkoušek bude ověřen soulad s definovanými normami a specifikacemi, především pak se specifikacemi C-ROADS Czech Republic. Dále bude ověřována funkčnost implementovaných služeb dle článku IV. Provedením komplexních testů těchto služeb bude zároveň prověřena funkčnost všech částí systému C2X jako celku.
- 4.5. Komplexní zkoušky budou prováděny v plném rozsahu instalované technologie C2X. Při testování jednotlivých implementovaných služeb musí být zvoleno vhodné místo s ohledem na daný a možnost opakovaného testování. Podkladem pro provedení komplexních testů budou testovací scénáře, které vypracuje Dodavatel na základě podkladů poskytnutých Zadavatelem. Dodavatel následně tyto testovací scénáře před započítím testů předloží Zadavateli ke schválení.

- 4.6. Výsledky komplexních zkoušek jednotlivých Use Cases budou zaznamenávány do připraveného záznamového archu, který bude obsahovat minimálně následující informace:
- Název případu užití (use case)
 - Typ scénáře
 - Výsledek zkoušky
 - Účastníci zkoušky
 - Podpis účastníků
 - Datum zkoušky
- 4.7. Pro provedení komplexních zkoušek vybraných služeb je nezbytná součinnost Zadavatele ve smyslu poskytnutí vozidla vybaveného OBU/RSU jednotkou.
- 4.8. **Školení.** V průběhu Etapy T1 je Dodavatel povinen vyškolit 3 zástupce Zadavatele na používání C-ITS systému v rozsahu obvyklém pro danou problematiku. Náklady související se zajištěním školení jsou součástí nabídkové ceny.
- 4.9. **Průběh Etapy T2.** Součástí dodávky je také Etapa T2. V rámci této etapy běží záruka na systém dle této technické specifikace, Zadavatel tento systém provozuje a provádí jeho běžnou údržbu a současně nabídne služby spojené s testováním Zadavatelem požadovaných scénářů v rámci C-ROADS Czech Republic a pilotního ověření ostatním členům konsorcia C-ROADS Czech Republic.
- 4.10. **Změny a rozšíření funkcionalit C-ITS systému.** V průběhu dodávky může Zadavatel rozhodnout o upřesnění, provedení úprav nebo rozšíření systému, které nejsou dostatečně přesně, popř. vůbec, popsány v této technické specifikaci, Dodavatel je povinen takové upřesnění, úpravy a rozšíření systému provést. Může se jednat např. o:
- rozšíření funkcionalit systému nad rámec této technické specifikace vyvolaných změnami zákonů, vyhlášek, technických podmínek, standardů atd. nebo z důvodu dodatečných požadavků Zadavatele plynoucích z užívání systému. Změny mohou být vyvolány také potřebami konsorcia C-ROADS Czech Republic, např. společná implementace postupů k naplnění evropského předpisu GDPR. Tyto změny budou realizovány v rámci alokovaných 100 člověkodnů, určených pro Etapu T2.

XV. SEZNAM ZKRATEK

Zkratka	Význam
APN	Access Point Name
ARM	Advanced RISC Machines (typ procesoru)
ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CALM	Communication Access for Land Mobiles
CAM	Cooperative Awareness Message
CEF	Connecting Europe Facility
CEN	European Committee for Standardization

C-ITS	Kooperativní ITS (Cooperative-ITS), někdy označováno jako C2X
C-ITS BO (back office)	Centrální systém C-ITS
C-ITS SIM	Dodávaný SW testovací nástroj určený V2X aplikace
CPU	Central Processing Unit (procesor)
CRL	Certificate Revocation List
CTL	Certificate Trust List
ČR	Česká republika
ČSN	Česká státní norma
DATEX II	Standard pro výměnu dopravních informací
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short-Range Communications
EEBL	Electronic Emergency Brake Light
EMC	Electromagnetic Compatibility
ETSI	European Telecommunications Standards Institute
EVA	Emergency Vehicle Approaching
GDPR	General Data Protection Regulation
GN	Geo Network
GNSS	Globální družicový polohový systém
GPIO	General Purpose Input/Output
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Grafické uživatelské rozhraní
HLN	Hazardous Location Notification
HMI	Human-Machine Interface
HSM	Hardware Security Module
HW	Hardware
I	Interface
I2V	Komunikace „infrastructure – vehicle“
ID	Identifikátor
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input / Output
IP	Integrační platforma
ISO	International Organization of Standardization
ISV	Intersection Signal Violation
ITS	Inteligentní dopravní systémy (Intelligent Transportation Systems)
ITS-G5	Evropská varianta technologie DSRC
IVI	In-Vehicle Information
IZS	Integrovaný záchranný systém
LŘD	Liniové řízení dopravy
LTE	Long Term Evolution
MAP	Map Data

MHD	Městská hromadná doprava
MIPS	Million Instruction Per Second
MMU	Memory Management Unit
MQTT	Message Queuing Telemetry Transport
NTP	Network Time Protocol
OBU	On-board unit
OSM	Open Street Map
PC	Personal Computer (Počítač)
PCAP	Packet Capture
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PTP	Public Transport Priority
PTS	Public Transport Safety
PVB	Probe Vehicle Data
RLX	Railway Level Crossing
RS232	Seriový port
RSU	Roadside Unit
RWW	Road Work Warnings
SIM	Subscriber Identification Module
SPAT	Signal Phase and Timing Message
SSM/SRM	Single Supervisory Mechanism / Single Resolution Mechanism
SSV	Slow and Stationary Vehicle
SSZ	Světlé signalizační zařízení
SW	Software
TJA	Traffic Jam Ahead
TLS	Transport Layer Security
TPM	Trusted Platform Module
UC (Use Case)	Případy užití, tj. popis scénářů pro užití v systému C-ROADS Czech Republic
USB	Rozhraní Universal Serial Bus
V2I	Komunikace „vehicle – infrastructure“
V2V	Komunikace „vehicle – vehicle“
V2X	Komunikace "vehicle – everything"
VPN	Virtual Private Network
WCW	Weather Conditions Warning
WG	Work Group
XML	Extensible Markup Language
ZD	Zadávací dokumentace
ZPI/PDZ	Zařízení pro provozní informace / proměnné dopravní značení