

C-ROADS CZ

Specifikace systému

Připraveno pracovní skupinou WG 2.1

Verze 2.0

12/2021



Verze	Datum změny	Autor	Kontrola	Komentář / popis změn
0.1	13.4.2017	INTENS		První pracovní verze dokumentu
0.2	27.4.2017	INTENS		Kapitoly 3 a 8
0.3	30.4.2017	ŘSD		Kapitoly 4.2, 5 a 6
0.4	9.5.2017	AŽD, RADOM		Doplnění kapitol 4 a 5
0.5	22.5.2017	O2		Doplnění kapitoly 4.1
0.6	22.5.2017	INTENS		Doplnění celého dokumentu
0.7	24.5.2017	INTENS/ČVUT		Doplnění kapitol 4 - 7
0.8	27.5.2017	INTENS		Doplnění celého dokumentu
0.9	29.5.2017	T-Mobile		Doplněny specifikace komunikačního rozhraní I4, I5
1.0	29.5.2017	ALL		Revize celého dokumentu
1.1	30.05.2018	INTENS		Formátování
1.2	17.07.2018	INTENS		Revize všech kapitol
1.4	14.12.2018	INTENS		Revize všech kapitol
1.5	31.1.2019	ALL		Revize všech kapitol
1.8	10.8.2021	INTENS		Revize všech kapitol
1.9	25.11.2021	INTENS		Revize všech kapitol, první draft finálních specifikací pro Release 2
2.0	17.12.2021	ALL		Revize všech kapitol

OBSAH

Seznam použitých zkratk	6
Zdroje	9
1 Úvod	11
2 Iniciativa C-Roads	12
2.1 Etapy implementace C-ROADS CZ	13
2.2 DT1 – D1 Brno	13
2.3 DT2 – Brno město	14
2.4 DT3 – Dálnice D1, D11, D5 a D52	15
2.5 DT4 – Dopravní podniky Ostrava a Plzeň	16
2.6 DT5 – Železniční křižení	18
2.7 DT6 – Přeshraniční testování	20
3 Vymezení závazných dokumentů	21
3.1 Legislativní rámec	21
3.1.1 Mezinárodní právní rámec	22
3.1.2 Právní rámec EU	22
3.1.3 Právní rámec ČR	25
3.2 Evropské standardy a normy	28
3.3 Harmonizované komunikační profily	31
3.3.1 C-Roads Platform	31
3.3.2 Car2Car Communication Consortium	32
3.4 Národní specifikace	32
3.5 Specifické požadavky	33
4 Ekosystém C-ITS	34
4.1 Centrální prvky C-ITS	35
4.1.1 Bezpečnostní vrstva – PKI	36
4.1.2 Integrovaná platforma	36
4.2 Centrální C-ITS stanice a informační zdroje	36
4.2.1 C-ITS Back Office	36
4.2.2 Informační zdroje	37
4.3 C-ITS stanice	38
4.3.1 C-ITS jednotky na infrastruktuře	38
4.3.2 C-ITS jednotky ve vozidlech	39
4.3.3 Mobilní aplikace	40
4.4 Přenosové komunikační technologie	41
4.4.1 ITS-G5	41



4.4.2	Mobilní datové sítě.....	42
4.4.3	Hybridní komunikace.....	42
4.5	Komunikační rozhraní mezi prvky systému.....	42
4.5.1	Rozhraní I1: vozidlové jednotky ↔ jednotky na infrastruktuře / vozidlové jednotky.....	44
4.5.2	Rozhraní I2: C-ITS Back Office ↔ C-ITS zařízení.....	49
4.5.3	Rozhraní I3: C-ITS Back Office ↔ Integrovaná platforma	51
4.5.4	Rozhraní I4: OBU ↔ vozidlové systémy.....	51
4.5.5	Rozhraní I5: RSU ↔ další zařízení na infrastruktuře	52
4.5.6	Rozhraní I6: C-ITS Back Office ↔ další informační zdroje	53
4.5.7	Rozhraní I7: C-ITS prvky ↔ PKI CZ	53
4.5.8	Rozhraní I8: PKI CZ ↔ PKI EU	53
5	Bezpečnost C-ITS systémů.....	55
5.1	Národní úroveň	56
5.1.1	Kořenová certifikační autorita.....	57
5.1.2	Registrační autorita.....	58
5.1.3	Autorizační autorita.....	58
5.2	Evropská úroveň.....	58
5.2.1	C-ITS Certificate Policy Authority.....	58
5.2.2	Trust List Manager.....	58
5.2.3	C-ITS Point of Contact	59
6	C-ITS služby.....	60

Seznam obrázků

Obrázek 1	Umístění RSU jednotek v rámci pilotní lokality DT1 (zdroj: Google.com).....	14
Obrázek 2	Umístění RSU jednotek v rámci pilotní lokality DT2 (zdroj: Google.com).....	15
Obrázek 3	Umístění RSU jednotek v rámci pilotní lokality DT3 – dálnice D5 (zdroj: Google.com).....	16
Obrázek 4	Umístění RSU jednotek v rámci pilotní lokality DT3 – dálnice D11 (zdroj: Google.com).....	16
Obrázek 5	Umístění RSU jednotek v rámci pilotní lokality DT4 - Plzeň (zdroj: Google.com)	17
Obrázek 6	Umístění RSU jednotek v rámci pilotní lokality DT4 - Ostrava (zdroj: Google.com)	18
Obrázek 7	Umístění RSU jednotek v rámci pilotní lokality DT5 – Pardubický kraj (zdroj: Google.com).....	19
Obrázek 8	Umístění RSU jednotek v rámci pilotní lokality DT5 – Ústecký kraj (zdroj: Google.com)	19
Obrázek 9	Funkční a technické specifikace zajišťující interoperabilní C-ITS systém	21
Obrázek 10	Architektura C-ITS SW stacku (zdroj: IEEE Communication Magazine, Vol. 53)	29
Obrázek 11	Vztah mezi harmonizovanými profily C2C-CC a C-Roads	31
Obrázek 12	Popis komponent ekosystému C-ITS (zdroj: Koncepce rozvoje C-ITS v ČR)	35
Obrázek 13	Rozhraní systému v rámci C-ITS ekosystému (zdroj: Koncepce rozvoje C-ITS v ČR)	44
Obrázek 14	Struktura zprávy CAM (zdroj: ETSI TS 102 637-2)	45



Obrázek 15 Struktura zprávy DENM (zdroj: ETSI TS 102 637-3).....	46
Obrázek 16 Struktura zprávy IVIM (zdroj: ISI/TS 19321).....	47
Obrázek 17 Struktura zprávy SPATEM (zdroj: ISO/TS 19091)	48
Obrázek 18 Struktura zprávy MAPEM (zdroj: ISO/TS 19091).....	48
Obrázek 19 Princip hybridního řešení	50
Obrázek 20 Základní schéma architektury bezpečnostní vrstvy (zdroj: Koncepce rozvoje C-ITS v ČR) ..	56

Seznam tabulek

Tabulka 1 Seznam závazných standardů a norem C-ITS.....	31
---	----

Seznam použitých zkratk

Zkratka	Význam
API	Application Programming Interface
APN	Access Point Name
ASECAP	European Association of Operators of Toll Road Infrastructures
BO	Back Office
BSD	Berkley Software Distribution
BTP	Basic Transport Protocol
CA	Certification Authority
CAM	Cooperative Awareness Message
CAN	Controller Area Network
CEF	Connecting Europe Facility
CEN	European Committee for Standardization
C-ITS	Kooperativní ITS (cooperative-ITS), někdy označováno jako C2X
C-ITS Back Office	Centrální systém C-ITS
ČR	Česká republika
DB	Databáze
DC	Direct current
DDS	Data Distribution Service
DENM	Decentralized Environmental Notification Message
DIC	Dopravní informační centrum
DP	Dopravní podnik
DPO	Dopravní podnik Ostrava
DT	Deployment and Tests
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
ECTL	European Certificate Trust List
ESB	Enterprise Service Bus
ETSI	European Telecommunications Standards Institute
GN	Geo Network
GNSS	Globální družicový polohový systém
GPS	Global Positioning System
GSM	Globální systém pro mobilní komunikaci
GUI	Grafické uživatelské rozhraní
HLN	Hazardous Location Notification
HMI	Human-Machine Interface
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
I	Interface
I2V	Komunikace „infrastructure – vehicle“

IEEE	Institute of Electrical and Electronics Engineers
IP	Integrační platforma
ISO	International Organization for Standardization
ITS	Inteligentní dopravní systémy (Intelligent Transportation Systems)
IVI	In vehicle information
JSDI	Jednotný systém dopravních informací
JŘ	Jízdní řád
LTE	Long Term Evolution
MAC	Media Access Control
MAP	Map Data
MDČR	Ministerstvo dopravy ČR
MHD	Městská hromadná doprava
MIRUD	Kooperativní ITS koridor Mirošovice - Rudná
NDIC	Národní dopravní informační centrum
NTP	Network Time Protocol
OBU	On-board unit
OMG	Object Management Group
OS	Operační systém
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PMDP	Plzeňské městské dopravní podniky
PPK	Požadavky na provedení a kvalitu na dálnicích a silnicích ve správě ŘSD ČR
PTP	Public Transport Preference
PTS	Public Transport Safety
PVD	Probe vehicle data
PVV	Protokoly o určení vnější vlivů
PZZ	Přejezdové zabezpečovací zařízení
RSU	Roadside unit
RVU	Road-Vehicle Unit
ŘDC	Řídicí dopravní centrum
ŘSD	Ředitelství silnic a dálnic
SIM	Subscriber Identity Module
SLA	Service-Level Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SP	Security Policy
SPAT	Signal Phase and Time
SSZ	Světelné signalizační zařízení
SW	Software
TCN	Tram Collision Notification
TLS	Traffic Light Status
TML	Trust List Mager
TP	Technické podmínky
TPM	Trusted Platform Module

UC	Use case
USB	Universal Serial Bus
Use case	Případy užití tj. popis scénářů pro užití v systému C-ROADS CZ
UTC	Coordinated Universal Time
V2V	Komunikace „vehicle – vehicle“
V2X	Komunikace "vehicle – everything"
VPN	Virtual Private Network
WAN	Wide Area Network
WDM	Wavelength-division Multiplexing
WiFi	Wireless Local Area Networking
WS	Web Services
XML	Extensible Markup Language

Zdroje

Číslo	Název
1.	Platné ETSI a ISO normy, viz kapitola 3.2
2.	C-Roads: Introduction to the C-Roads WG2 Deployment Documentation and Requirements
3.	C-Roads: C-ITS Security Requirements and Specifications
4.	C-Roads: C-ITS Security and Governance
5.	C-Roads: C-ITS Service and Use Case Definitions
6.	C-Roads: C-ITS Message Profiles and Parameters
7.	C-Roads: C-ITS Mobile Roadside ITS G5 System Profile
8.	C-Roads: C-ITS Roadside ITS G5 System Profile
9.	C-Roads: C-ITS IP Based Interface Profile
10.	C-ROADS CZ: Use Case katalog
11.	C-ROADS CZ: Interface Contract BO2BO
12.	C-ROADS CZ: C-Roads Security Concept
13.	CAR 2 CAR Communication Consortium: Basic System Profile 1.6.0
14.	Platform for the deployment of C-ITS in the EU, Final report [EK, 1/2016]
15.	COM (2016) 766 – A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility
16.	SCOOP@F Specification [2016]
17.	Architecture for C-ITS applications in the Netherlands v.1.0 [Igor Passchier (TASS), Marcel van Sambeek (TNO) 2016]
18.	Eco-AT Release 6 documents European Corridor – Austrian Testbed for Cooperative Systems, version 3.00 (SWP 2.1 – 3.7), [AustraTech 2017]
19.	Metodika zavádění kooperativních ITS v ČR; [MDČR 2013]
20.	Návrh otevřené národní platformy ITS koridoru a její realizace na části dálniční sítě v ČR; [ŘSD ČR 2015]
21.	Guide about technologies for future C-ITS service scenarios [ERTICO 2015]
22.	Roadmap between automotive industry and infrastructure organizations on initial deployment of Cooperative ITS in Europe v 1.0 [Amsterdam Group 2013]
23.	Amsterdam Group ITS [online] www.amsterdamgroup.eu

24.	C-ITS Platform: Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (CP) [2017]
25.	C-ITS Platform: Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (SP) [2017]
26.	Koncepce rozvoje C-ITS v ČR [2021]
27.	Task 48.3 - Action Plan: Centrální prvky C-ITS [2021]
28.	Integrační platforma – Dokumentace pro připojení subjektů

1 Úvod

Tento dokument slouží jako základní funkční a technický popis jednotlivých komponent C-ITS systému a jejich vzájemného komunikačního propojení, který byl vytvořen za účelem úspěšné realizace projektu C-Roads Czech Republic (zkráceně C-ROADS CZ), který je součástí pan-evropské platformy C-Roads. Cílem této platformy je zajistit interoperabilitu budovaných C-ITS systémů v Evropě a C-ROADS CZ je jedním z projektů, které se budou v rámci této platformy realizovat. Více informací o tomto projektu je uvedeno v kap. č. 2.

Tento dokument stanovuje základní fyzickou a komunikační architekturu, principy a pravidla pro budování C-ITS systémů. Tyto technické a funkční požadavky byly vytvořeny partnery projektu C-ROADS CZ a vychází ze zkušeností s implementací a provozem C-ITS systémů nejen českých, ale i zahraničních partnerů. Tento dokument zároveň slouží jako návod dalším zájemcům o budování C-ITS systému pro zajištění kompatibility a interoperability celého systému na národní a mezinárodní úrovni. Tento dokument tak představuje možný podklad pro případnou technickou specifikaci zadávacích dokumentací na implementaci C-ITS systémů do různých prostředí v rámci České republiky.

Tento dokument nepopisuje všechny požadavky na C-ITS systém v největší hloubce detailu a snaží se definovat základní rámec pro zajištění interoperability systému a nastavení otevřené architektury pro snadné rozšiřování a úpravy dle aktuálních potřeb. Tento dokument byl v jednotlivých fázích projektu průběžně aktualizován na základě poznatků z implementace systémů do běžného provozu.



2 Iniciativa C-Roads

Iniciativa C-Roads byla vytvořena jakožto společná platforma členských států spolupracujících na vývoji harmonizovaných a interoperabilních kooperativních systémů v Evropském prostoru. Platforma je zaměřena na spolupráci členských států, sdílení zkušeností a znalostí. Pro práci byl zvolen tzv. bottom-up koncept, jehož součástí jsou pilotní ověření C-ITS na národních úrovních. Tyto systémy následně tvoří základ pro pozdější panevropskou implementaci C-ITS. Národní iniciativy dále přerostly v tzv. cross-site testování, kde byla ověřena mezinárodní interoperabilita.

Projekt C-Roads Czech Republic je úzce spojený s mezinárodní iniciativou C-Roads, jež byla výsledkem společné aktivity států ČR, Rakouska a Německa, ke které se později připojily i další evropské státy.. Platforma C-Roads si klade za cíl harmonizaci a spolupráci při zavádění systémů C-ITS napříč Evropou. Projekt je spolufinancován z Nástroje pro propojení Evropy (CEF Transport) z víceletého pracovního programu Evropské unie. Celá aktivita na české národní úrovni je koordinována Ministerstvem dopravy, které je zároveň zřizovatelem prováděcího subjektu ŘSD ČR odpovědného za implementaci C-ITS systémů na dálnice a silnice I. třídy. Dalšími partnery projektu jsou:

- Správa železnic (SŽ),
- Brněnské komunikace (BKOM),
- České vysoké učení technické – Fakulta dopravní (ČVUT FD),
- O2 Czech Republic (O2),
- T-Mobile Czech Republic (TMCZ),
- INTENS Corporation (INTENS),
- AŽD Praha (AŽD).

Cíle projektu vycházely z výsledků a doporučení závěrečné zprávy zpracované platformou Evropské komise pro kooperativní systémy dne 21. ledna 2016 a naplňovaly opatření z cílů Akčního plánu rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050) schváleného usnesením vlády ze dne 15. dubna 2015 č. 268.

V rámci tohoto projektu bylo výrazně rozšířeno pokrytí C-ITS koridoru ze silničního okruhu kolem Prahy (SOKP) po dálnici D5 do Plzně a po dálnici D11 do Hradce Králové. Dále byla vybavena část dálnice D1 v okolí Brna. Projekt však nebyl zaměřen pouze na dálnice, ale věnoval se i implementaci C-ITS technologie do měst (Plzeň, Brno, Ostrava).

V rámci projektu bylo také testováno využití systémů C-ITS v městské hromadné dopravě, a to konkrétně v Plzni, Brně a Ostravě, kde se dopravní podniky zavázaly poskytnout pro účely testování svá vozidla a infrastrukturu. Zároveň byly testovány služby spojené s železničními přejezdy, přičemž organizace SŽ vyčlenila pro tyto účely čtyři zabezpečené přejezdy v Pardubickém a Ústeckém kraji s cílem zvýšit bezpečnost, a snížit tak počet zraněných a usmrcených lidí v důsledku střetu vlaku se silničním dopravním prostředkem informováním řidičů vozidel v blízkém okolí přejezdu o blížícím se vlaku.



Rozsah jednotlivých pilotních lokalit v rámci projektu C-Roads Czech Republic je popsán v podkapitole níže.

2.1 Etapy implementace C-ROADS CZ

Návrh implementace projektu C-ROADS CZ byl v pracovní skupině WG2.2 geograficky i časově rozdělen do 6 základních částí pojmenovaných DT1 – DT6, kde:

- DT1 Brno – odpovědnost za řešení mají partneři ŘSD ČR, O2, T-Mobile, BKOM
- DT2 Brno město – odpovědnost za řešení mají partneři BKOM, ŘSD ČR, O2, T-Mobile
- DT3 dálnice D1/D11/D5/D52 – odpovědnost za řešení mají partneři ŘSD ČR, O2, T-Mobile
- DT4 města Ostrava/Plzeň – odpovědnost za řešení mají partneři INTENS, O2, T-Mobile a asociovaní partneři Dopravní podnik Ostrava a.s. a Plzeňské městské dopravní podniky a.s.
- DT5 železniční křižení – odpovědnost za řešení mají partneři SŽ, AŽD, a ŘSD ČR
- DT6 přeshraniční testování – zapojení zahraničních partnerů, ŘSD ČR, O2, T-Mobile

Bližší popis jednotlivých implementačních etap je uveden v textu níže.

2.2 DT1 – D1 Brno

Tato pilotní lokalita zahrnuje úsek dálnice D1 kolem Brna (délka úseku je přibližně 28 km, staničení km 182 až km 210) společně s hlavními silničními přívaděči do centra města z dálnice D1.

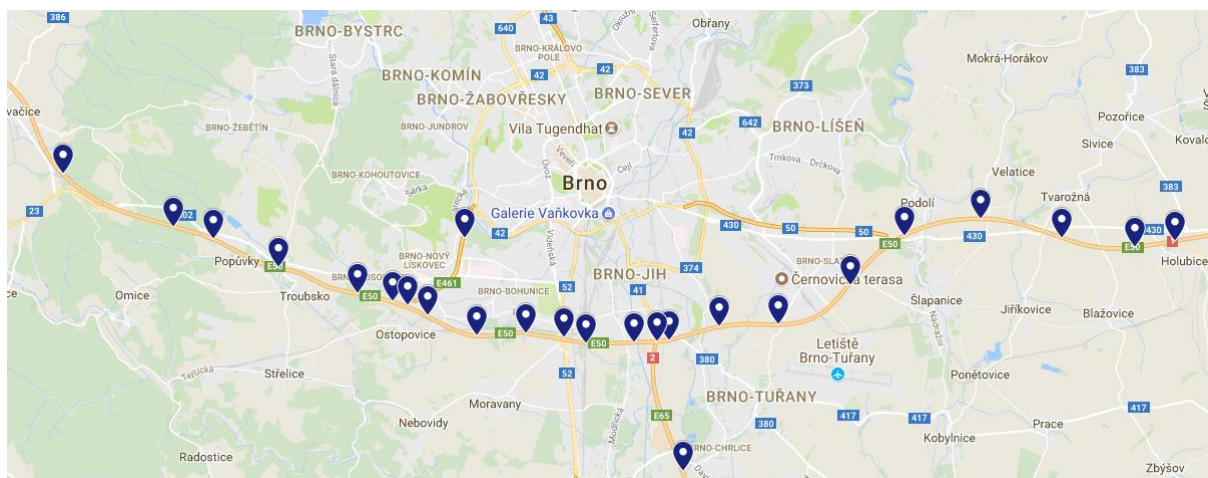
Celkově bylo na této lokalitě instalováno 25 RSU jednotek (společně s BT a WiFi detektory), které byly umístěny jak na stávající konstrukce (veřejné osvětlení, info portál ZPI/PDZ, stožár CCTV, silniční meteorologická stanice, portál dopravního značení), tak na nové stožáry u SOS hlásek vybudovaných v rámci této dodávky. Dále bylo vozidlovými jednotkami vybaveno 39 vozidel a 30 zabezpečovacích vozíků ve správě SSÚD Brno-Chrlice. Dalšími vozidlovými C-ITS jednotkami byla vybavena vozidla partnerů projektu (včetně asociovaných partnerů), která byla použita pro testovací účely. Veškerá tato C-ITS zařízení jsou propojena s C-ITS BO ŘSD.

Na této lokalitě měly být realizovány minimálně následující C-ITS služby:

- Road Works Warning
- Probe Vehicle Data
- In-Vehicle Information
- Slow and Stationary Vehicle
- Emergency Vehicle Approaching

V rámci zakázky na implementaci C-ITS technologie na pilotní lokalitu DT1 byla vytvořena i mobilní aplikace pro HMI zařízení, která podporuje všechny C-ITS služby definované v rámci projektu C-Roads.





Obrázek 1 Umístění RSU jednotek v rámci pilotní lokality DT1 (zdroj: Google.com)

2.3 DT2 – Brno město

V rámci této pilotní lokality byly RSU jednotky instalovány na předdefinované lokality na Velkém městském okruhu (VMO), komunikacích propojujících VMO a dálnici D1 a na některých dalších křižovatkách. Na těchto lokalitách bylo nasazeno celkem 31 RSU jednotek, zejména do oblastí křižovatek. Tyto jednotky jsou zároveň propojeny s řadiči světelné signalizace. C-ITS systém je tak schopen identifikovat jízdu na signál „stůj“ a zvýšit tak bezpečnost na křižovatkách.

Částí projektu bylo i vybavení vozidel údržby v Brně (BKOM) 10 vozidlovými C-ITS jednotkami a jedna vozidlová C-ITS jednotka byla nainstalována do vozidla Hasičského záchranného sboru Jihomoravského kraje (HZS). Dalšími 2 vozidlovými C-ITS jednotkami byla vybavena vozidla partnerů projektu (včetně asociovaných partnerů), která byla použita pro testovací účely. Dále byl v rámci této aktivity vytvořen lokální C-ITS Back Office. Tento C-ITS Back Office shromažďuje veškerá data v rámci C-ITS systému ve městě, ovládá C-ITS zařízení ve městě a sdílí předdefinovaná data s ostatními C-ITS Back Offices prostřednictvím Integrovaní platformy.

Do této pilotní lokality se také zapojil Dopravní podnik města Brna, který poskytl svou C-ITS infrastrukturu a vozidla pořízená v rámci jiného projektu pro testování vzájemné interoperability v rámci služby preference MHD.

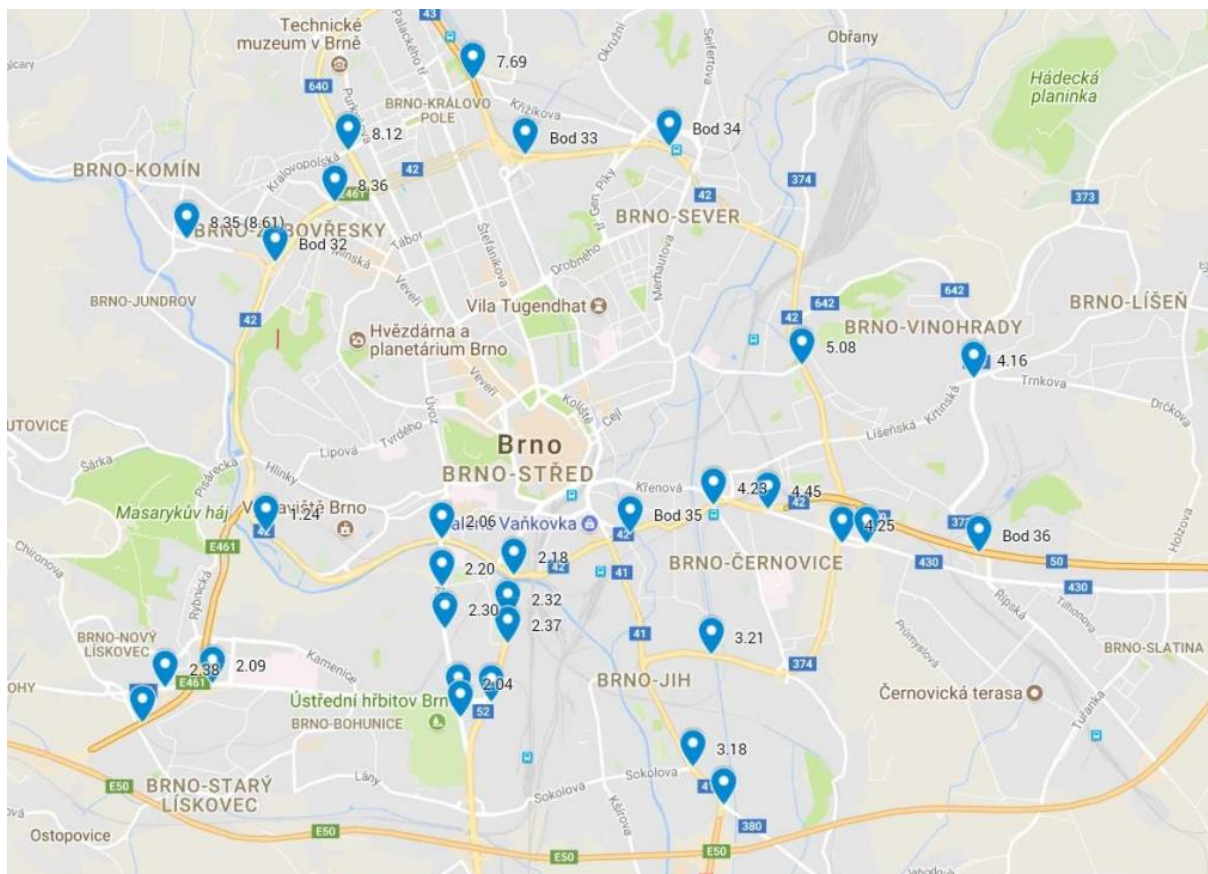
Na této lokalitě měly být realizovány minimálně tyto C-ITS služby:

- Probe Vehicle Data
- Emergency Vehicle Approaching
- Intersection Signal Violation
- Weather Conditions Warning
- Road Works Warning
- Hazardous Location Notification



- Public Transport Preference

V rámci zakázky na implementaci C-ITS technologie na pilotní lokalitu DT2 byla vytvořena i mobilní aplikace pro HMI zařízení, která podporuje všechny služby definované v rámci projektu C-Roads.



Obrázek 2 Umístění RSU jednotek v rámci pilotní lokality DT2 (zdroj: Google.com)

2.4 DT3 – Dálnice D1, D11, D5 a D52

Etapu DT3 lze dále rozdělit na dvě části podle použití přenosové technologie. Na části úseků dálnic D1, D11, D5 a D52 byla nasazena a použita primárně technologie ITS-G5, pro zbylou část vybraných úseků byly pro přenos varovných/informačních zpráv použity výhradně datové služby mobilních operátorů.

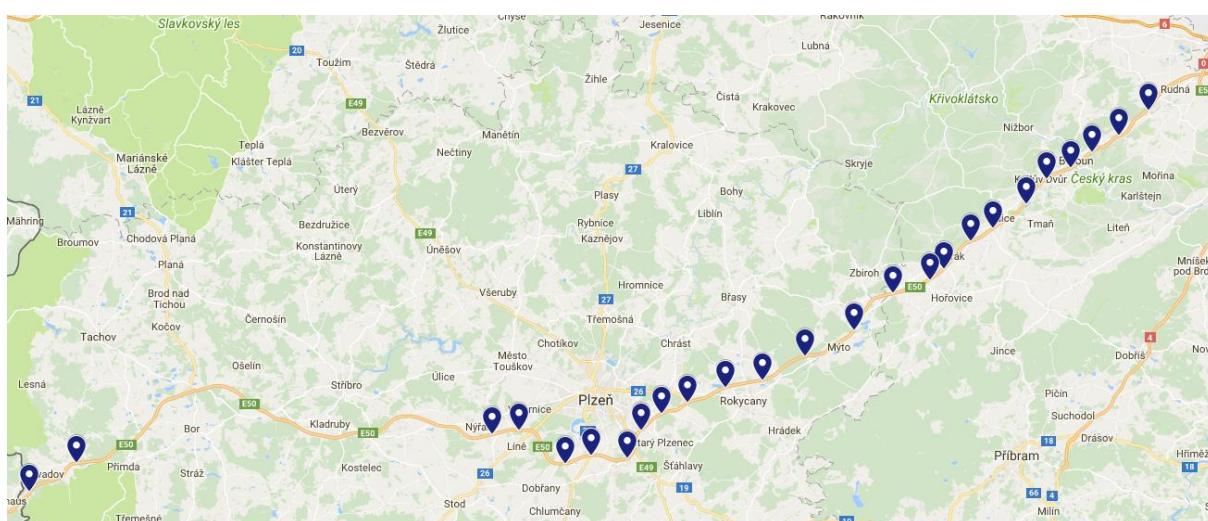
Přenosová technologie ITS-G5 byla nasazena na dálnici D11 v úseku Praha – Hradec Králové, na úsek dálnice D5 mezi Prahou a Plzní a do oblasti hraničního přechodu Rozvadov pro účely přeshraničního testování. Celkem bylo na těchto úsecích nainstalováno 54 RSU jednotek společně s BT a WiFi detektory.

Na ostatních úsecích vybraných dálničních úseků jsou C-ITS služby poskytovány prostřednictvím datových služeb mobilních operátorů. Celková délka pokrytých úseků v rámci etapy DT3 je více než 360 km.

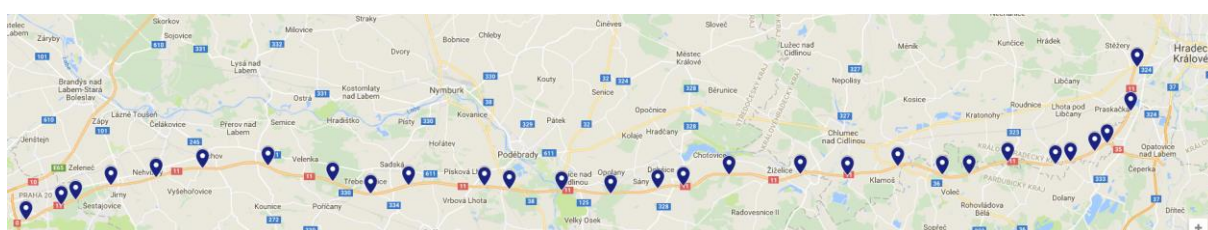
V této části projektu bylo instalováno 70 vozidlových C-ITS jednotek do vozidel v majetku ŘSD a 94 vozidlových jednotek do zabezpečovacích vozíků a dalšími 5 vozidlovými C-ITS jednotkami byla vybavena vozidla partnerů projektu (včetně asociovaných partnerů), která byla použita pro testovací účely. Všechny C-ITS zařízení v rámci této etapy jsou propojena s C-ITS Back Office ŘSD.

Na této lokalitě měly být kompletně realizovány minimálně tyto C-ITS služby:

- Road Works Warning
- Probe Vehicle Data
- Slow and Stationary Vehicle



Obrázek 3 Umístění RSU jednotek v rámci pilotní lokality DT3 – dálnice D5 (zdroj: Google.com)



Obrázek 4 Umístění RSU jednotek v rámci pilotní lokality DT3 – dálnice D11 (zdroj: Google.com)

2.5 DT4 – Dopravní podniky Ostrava a Plzeň

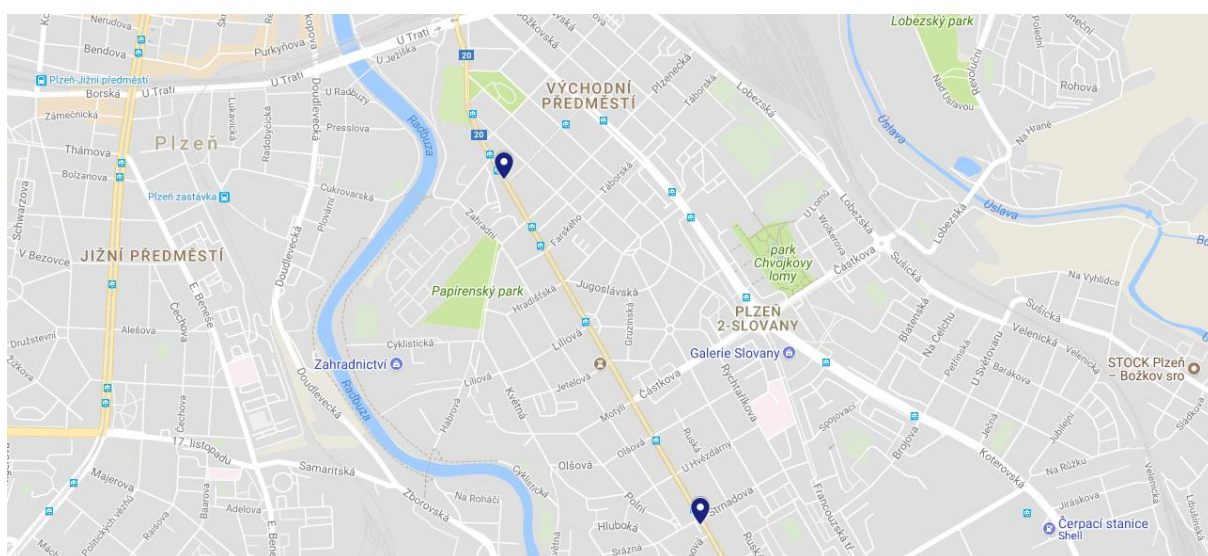
V Ostravě a v Plzni byly testovány C-ITS služby zaměřené na městskou hromadnou dopravu. V rámci této etapy byla testována prioritizace jízdy vozidel MHD na křižovatkách řízených SSZ prostřednictvím technologie ITS-G5 nebo upozornění řidičů na přítomnost vozidel MHD zejména na křižovatkách, kde hrozí největší nebezpečí srážky při křižovatkových manévrech (např. křížení tramvajové trati při levém odbočení vozidla). V rámci této aktivity byly dočasně nainstalovány 4 C-ITS vozidlové jednotky do

vozidel v majetku PMDP a 5 jednotek do vozů v majetku DPO. V rámci DT4 byly v Plzni instalovány 2 RSU jednotky, které byly propojeny s řadičem SSZ. V Ostravě bylo nainstalováno 5 RSU jednotek.

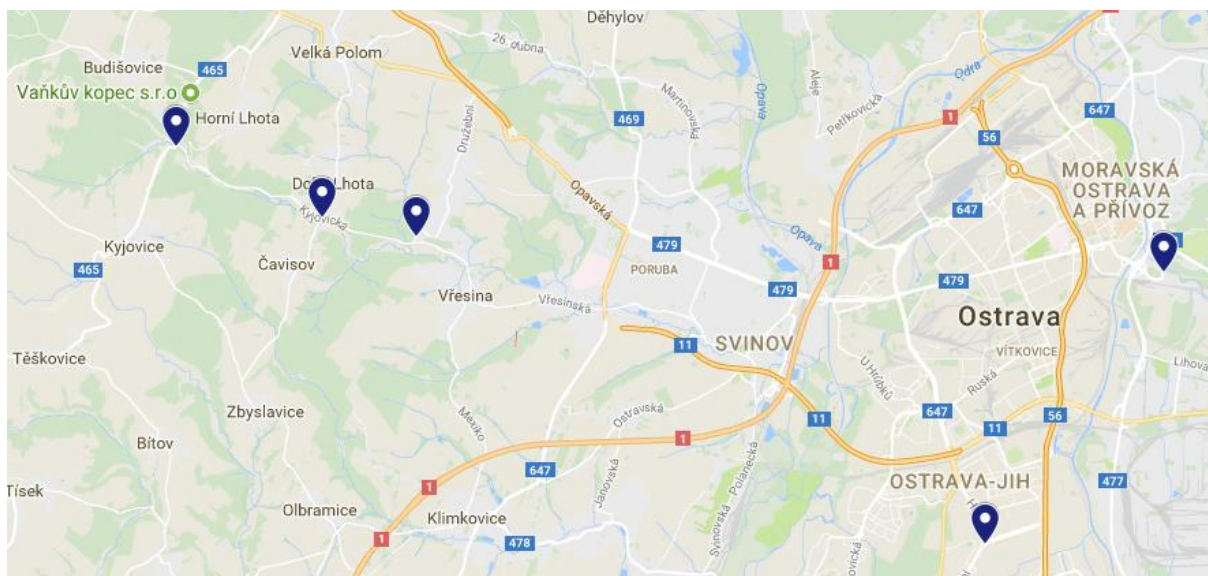
Na této lokalitě měly být testovány minimálně tyto C-ITS služby:

- Public Transport Preference
- Public Transport Safety
- Hazardous Location Notification
- Probe Vehicle Data
- Tram Collision Notification
- Traffic Light Status

V rámci implementace technologie byla navíc vytvořena mobilní aplikace pro HMI zařízení, která podporuje všechny služby definované v rámci projektu C-Roads, a také lokální C-ITS Back Offices, samostatný pro každé z měst. Tyto C-ITS Back Offices shromažďovaly veškerá data v rámci C-ITS systému ve městě, ovládaly C-ITS zařízení ve městě a sdílely předdefinovaná data s ostatními C-ITS Back Offices prostřednictvím Integrovaní platformy.



Obrázek 5 Umístění RSU jednotek v rámci pilotní lokality DT4 - Plzeň (zdroj: Google.com)



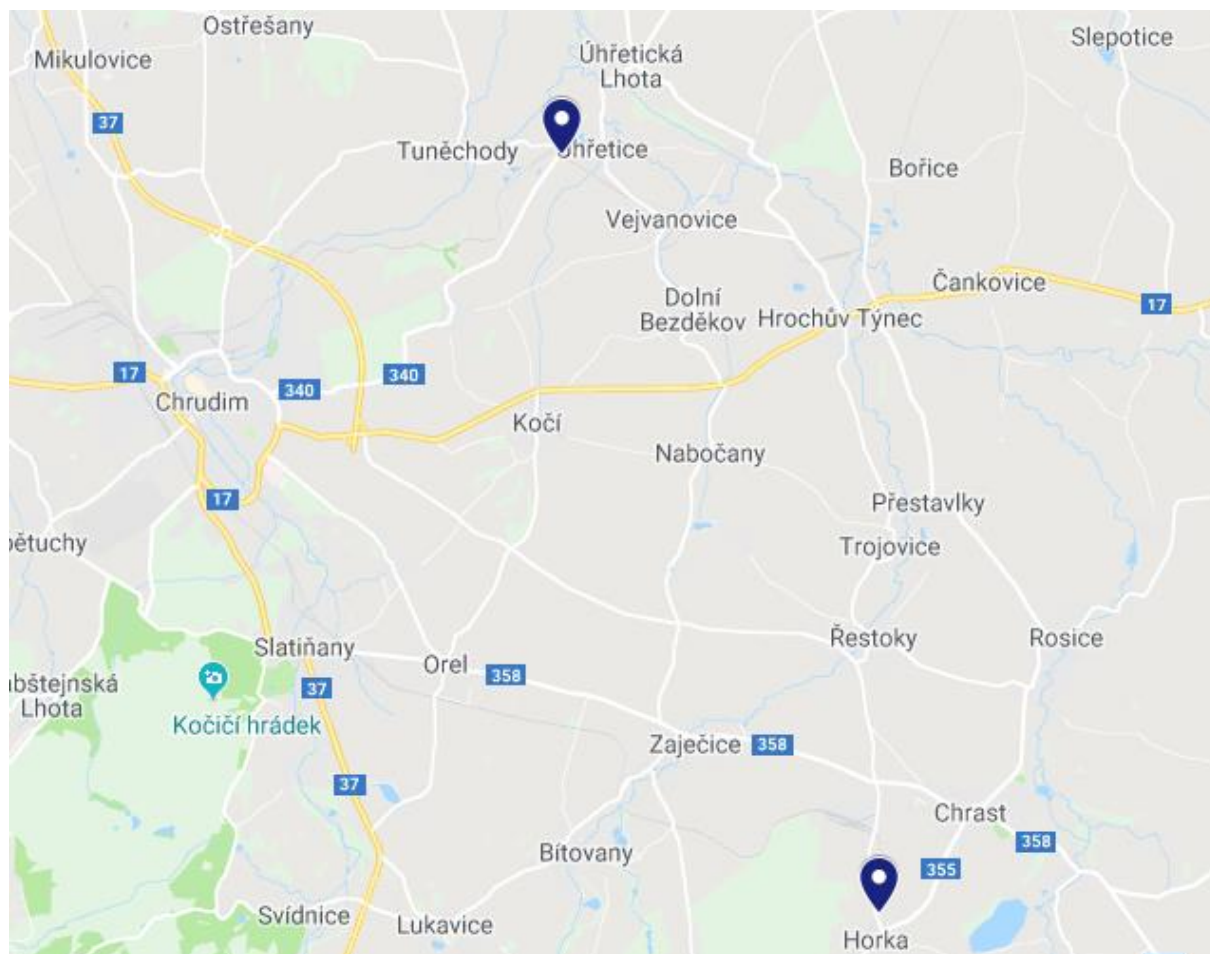
Obrázek 6 Umístění RSU jednotek v rámci pilotní lokality DT4 - Ostrava (zdroj: Google.com)

2.6 DT5 – Železniční křížení

Testování C-ITS systému na železničních přejezdech bylo prováděno v Pardubickém kraji (železniční tratě „Heřmanův Městec – Moravany“ a Pardubice, „Rosice nad Labem – Žďárec u Skutče“), kde byla ITS-G5 technologie nasazena na dva vybrané železniční přejezdy s přejezdovým zabezpečovacím zařízením, a v Ústeckém kraji (železniční trať „Čížkovice – Obrnice“) byly C-ITS systémem osazeny dva železniční přejezdy. V rámci této aktivity bylo vybaveno i několik vozidel partnerů projektu jednotkou OBU pro otestování funkčnosti systému. Cílem testování bylo ověřit use case varování řidiče před úrovnovým železničním přejezdem a tím pádem zvýšit bezpečnost na železničních přejezdech. Řidič byl zároveň na této pilotní lokalitě upozorňován na přítomnost stojícího vozidla před přejezdem.

Na této lokalitě měly být testovány minimálně tyto C-ITS služby:

- Railway Level Crossing
- Slow and Stationary Vehicle



Obrázek 7 Umístění RSU jednotek v rámci pilotní lokality DT5 – Pardubický kraj (zdroj: Google.com)



Obrázek 8 Umístění RSU jednotek v rámci pilotní lokality DT5 – Ústecký kraj (zdroj: Google.com)

2.7 DT6 – Přeshraniční testování

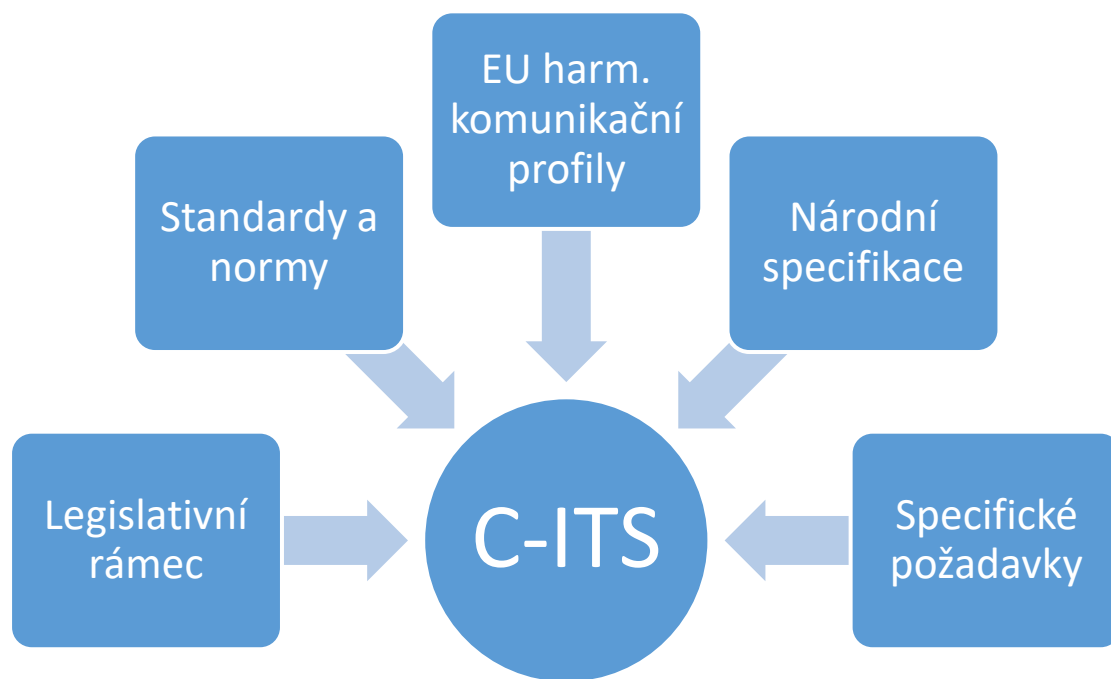
V rámci této části projektu byla testována interoperabilita C-ITS služeb navržených v rámci projektu C-ROADS CZ. Geografický i technický rozsah testování byl definován v rámci C-Roads Platformy (TF5) a také bilaterálním jednáním s ostatními státy C-Roads. Průběh testování byl shrnut v dokumentu „C-ITS Cross-Border Testing Report – C-Roads Czech Republic“.

3 Vymezení závazných dokumentů

Tato kapitola vymezuje závazné legislativní a technické dokumenty a doporučení v oblasti dalšího rozvoje přenosových komunikačních technologií a komunikačních rozhraní mezi jednotlivými komponentami C-ITS.

Při budování a implementaci C-ITS systémů do běžného provozu se nestačí řídit pouze evropskými normativními dokumenty, ale je nezbytné řídit se zároveň také evropskými harmonizovanými komunikačními profily, které zajišťují interoperabilitu zařízení různých výrobců a zároveň jednotně definují poskytované C-ITS služby, aby uživatel obdržel stejně kvalitní informace na celém území členských států. Další skupinou požadavků a omezení, které mohou být při budování C-ITS systému důležité, jsou evropské/národní zákony a vyhlášky a specifické požadavky konkrétních subjektů.

Skupiny požadavků a omezení, které mohou mít vliv na budování C-ITS systémů jsou uvedeny v obrázku níže.



Obrázek 9 Funkční a technické specifikace zajišťující interoperabilní C-ITS systém

3.1 Legislativní rámec

Tato kapitola uvádí legislativní dokumenty týkající se implementace a provozu C-ITS systémů z pohledu mezinárodního, evropského a národního práva. Vymezený právní rámec se netýká pouze systémů budovaných během projektu C-ROADS CZ, ale i systémů budovaných po skončení projektu. Účelem této kapitoly je informovat dodavatele C-ITS systémů a zadavatele připravující zadávací dokumentaci

o dostupných dokumentech, které se daného tématu C-ITS dotýkají. Jedná se tedy pouze o strukturovaný výčet dokumentů dle, které nejsou detailněji interpretovány.

Legislativní rámec lze rozdělit do následujících kategorií:

- Mezinárodní právní rámec
- Právní rámec EU
 - Nařízení
 - Směrnice
 - Rozhodnutí
 - Strategické dokumenty, které nejsou závazné
- Právní rámec ČR
 - Zákony
 - Vyhlášky
 - Usnesení vlády ČR

3.1.1 Mezinárodní právní rámec

V ústavě ČR je zakotven přednost mezinárodních smluv před zákony ČR v případě, kdy byl k ratifikaci mezinárodních smluv udělen souhlas Parlamentu ČR. Mezi mezinárodní smlouvy, které tak mohou mít vliv na C-ITS patří zejména:

- Úmluva o silničním provozu (tzv. Vídeňská úmluva z roku 1968), která tvoří základní mezinárodní smlouvu o podobě silniční dopravy, když stanoví jednotná pravidla mezinárodního silničního provozu.
- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108, vyhlášená pod č. 115/2001 sb. Předmětem je snaha zaručit na území každé smluvní strany každé fyzické osobě, ať je jakékoli národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují.

3.1.2 Právní rámec EU

Česká republika musí respektovat i právo Evropské unie. Rozvoj C-ITS probíhá v celé EU a to i na legislativní úrovni, předpokladem pro vznik jednotného C-ITS je harmonizace napříč EU.

Základními právními předpisy, které ovlivňují rozvoj C-ITS jsou:

- Nařízení
- Směrnice
- Rozhodnutí
- Další dokumenty vydané EU, které nemají závazný charakter



3.1.2.1 Nařízení

Nařízení, která mohou ovlivňovat ekosystém C-ITS jsou následující:

- Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („Akt o kybernetické bezpečnosti“);
- Nařízení komise v přenesené pravomoci (EU) 2017/1926 ze dne 31. května 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU, pokud jde o poskytování multimodálních informačních služeb o cestování v celé Unii;
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále také „Nařízení GDPR“);
- Nařízení Komise v přenesené pravomoci (EU) 2015/962 ze dne 18. prosince 2014, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU, pokud jde o poskytování informačních služeb o dopravním provozu v reálném čase v celé EU;
- Nařízení Komise (EU) č. 1305/2014 ze dne 11. prosince 2014 o technické specifikaci pro interoperabilitu subsystému „Využití telematiky v nákladní dopravě“ železničního systému Evropské unie a o zrušení nařízení (ES) č. 62/2006;
- Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy;
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále také „Nařízení eIDAS“). Nařízení eIDAS mimo jiné definuje pojem elektronický podpis, který se užívá i v bezpečnostní vrstvě PKI;
- Nařízení Komise (EU) č. 1273/2013 ze dne 6. prosince 2013, kterým se mění nařízení (EU) č. 454/2011 o technické specifikaci pro interoperabilitu týkající se subsystému „využití telematiky v osobní dopravě“ transevropského železničního systému;
- Nařízením Evropské komise v přenesené pravomoci (EU) 886/2013 ze dne 15. 5. 2013, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU. Nařízení mimo jiné definuje minimální univerzální informace o dopravním provozu, které by měly být poskytovány bezplatně, pokud je to možné tak, aby mohly být šířeny, co největšímu okruhu řidičů. Dopravní informace mají být poskytovány bezplatně, což ale neznamená, že zdarma, tzn. můžou být zohledněny náklady spojené se sběrem a zpracováním informací;
- Nařízení Komise v přenesené pravomoci (EU) č. 885/2013 ze dne 15. května 2013, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU o inteligentních



dopravních systémech, pokud jde o poskytování informačních služeb týkajících se bezpečných a chráněných parkovacích míst pro nákladní a užitková vozidla;

- Nařízení Evropského parlamentu a Rady (ES) č.1072/2009, o společných pravidlech pro přístup na trh mezinárodní silniční nákladní dopravy;
- Nařízení Evropského parlamentu a Rady (ES) č. 1071/2009 ze dne 21. října 2009, kterým se zavádějí společná pravidla týkající se závazných podmínek pro výkon povolání podnikatele v silniční dopravě a zrušuje směrnice Rady 96/26/ES.;
- Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93;
- Nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy, o změně nařízení Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a o zrušení nařízení Rady (EHS) č. 3820/85.

Po vytvoření harmonizovaných komunikačních profilů (viz kap. č. 3.3) platformou C-Roads a konsorciem Car2Car byla snaha legislativně ukotvit tyto specifikace prostřednictvím nařízení EK v přenesené pravomoci (tzv. „delegovaného aktu“) k systémům C-ITS. Tento dokument tak měl stanovit pravidla pro využívání stávajících a rozvojových C-ITS technologií (v době vzniku dokumentu ITS-G5 a LTE) a nikterak neomezovat rozvoj a budoucí nasazení jiných technologií. Tento dokument však nebyl schválen všemi členskými státy EU. Z toho důvodu vznikla asociace C-ITS Deployment Group, která sdružuje výrobce vozidel, správce dopravní infrastruktury a další subjekty, které podporují jednotný rozvoj C-ITS v Evropě a jsou v souladu s harmonizovanými komunikačními profily. Mezi členy této asociace patří i partneři projektu C-ROADS CZ.

3.1.2.2 Směrnice

Směrnice, které mohou ovlivňovat ekosystém C-ITS jsou následující:

- Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru;
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Směrnice mimo jiné stanoví požadavky ohledně vnitrostátních schopností v oblasti kybernetické bezpečnosti, zřizuje mechanismy pro posílení strategické a operativní spolupráce mezi členskými státy a zavádí povinnosti v oblasti bezpečnostních opatření a hlášení incidentů v různých odvětvích;
- Směrnice Evropského parlamentu a Rady 2010/40/EU ze dne 7. července 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy. Směrnice mimo jiné definuje povinnost zajistit, aby budované i již zavedené systémy a aplikace ITS dosáhly odpovídající míry kompatibility a interoperability nejen po



technické, ale i po organizační stránce, a to včetně posouzení shody nebo vhodnosti pro použití v souladu s touto specifikací;

- Směrnice Evropského parlamentu a Rady 2007/46/ES ze dne 5. září 2007, kterou se stanoví rámec pro schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla;
- Směrnice Evropského parlamentu a Rady 2004/52/ES ze dne 29. dubna 2004 o interoperabilitě elektronických systémů pro výběr mýtného ve Společenství;
- Směrnice Rady 85/374/EHS ze dne 25. července 1985 o sblížování právních a správních předpisů členských států týkajících se odpovědnosti za vadné výrobky doplněnou Směrnicí Rady 99/34/ES.

3.1.2.3 Rozhodnutí

Rozhodnutí, která mohou ovlivňovat ekosystém C-ITS jsou následující:

- Rozhodnutí Komise EU 2020/1426 ze dne 7. října 2020 o harmonizovaném využívání rádiového spektra v kmitočtovém pásmu 5 875–5 935 MHz pro aplikace inteligentních dopravních systémů (ITS) související s bezpečností;
- Rozhodnutí Komise 2009/750/ES ze dne 6. října 2009 o definici evropské služby elektronického mýtného a jejích technických prvků.

3.1.2.4 Strategické dokumenty

Mezi další dokumenty, které byly vydané v rámci EU a mohou ovlivňovat ekosystém C-ITS patří:

- COM/2020/66 Evropská strategie pro data;
- COM/2016/0766 final "A European strategy on Cooperative Intelligent Transport Systems, a first milestone towards cooperative, connected and automated mobility;
- COM/2016/588 final „5G for Europe: An Action Plan“. Předmětem dokumentu je mimo jiné podpora technologií 5G, jejich testování a zavádění. Pokrytí sítí 5G je předpokládáno v městské zástavbě a na hlavních tazích do roku 2025;
- COM/2011/144 Plán jednotného evropského dopravního prostoru – vytvoření konkurenceschopného dopravního systému účinně využívajícího zdroje.

Tyto dokumenty nejsou závazné a mají pouze doporučující charakter.

3.1.3 Právní rámec ČR

Právní akty, které mají vliv na zavádění C-ITS systémů jsou:

- Zákony
- Vyhlášky
- Usnesení Vlády ČR



- Další národní strategické dokumenty

3.1.3.1 Zákony

Zákony, které mohou ovlivňovat ekosystém C-ITS jsou následující:

- Zákon č. 110/2019 Sb., o zpracování osobních údajů a zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů;
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen Zákon o kybernetické bezpečnosti). Doprava je podle § 2 písm. i) zákona č. 181/2014 Sb. o kybernetické bezpečnosti zařazena mezi tzv. základní služby, jejichž fungování je závislé na fungování elektronických komunikací nebo informačních systémech a jejichž narušení by mohlo být významný dopad na zabezpečení společenských a ekonomických činností;
- Zákon č. 89/ 2012 Sb., občanský zákoník v platném znění, účinnost plánována od 1. 1. 2014 („Občanský zákoník“);
- Zákon č. 40/2009 Sb., trestní zákoník, v platném znění;
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů;
- Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů;
- Zákona 56/2001 Sb. o podmínkách provozu vozidel na pozemních komunikacích;
- Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů, ve znění pozdějších předpisů (dále také „Zákon o provozu na pozemních komunikacích“). Důležitým bodem zákona je §124 odst. 3, podle kterého Ministerstvo dopravy nebo jím pověřená osoba zajišťuje informovanost veřejnosti o situacích v provozu na pozemních komunikacích, které mají vliv na bezpečnost a plynulost provozu na pozemních komunikacích. Za tím účelem jsou policie, obecní policie, silniční správní úřady, správci pozemních komunikací a Hasičský záchranný sbor povinni poskytovat ministerstvu aktuální informace, které mají vliv na bezpečnost a plynulost provozu na pozemních komunikacích. Prováděcí právní předpis stanoví druh informací, které mají vliv na bezpečnost a plynulost silničního provozu, způsob předávání informací, způsob sběru informací a způsob zveřejňování informací pro potřeby dopravní veřejnosti;
- Zákon č.218/2000 Sb., o rozpočtových pravidlech. K zákonu č.218/2000 Sb., o rozpočtových pravidlech musí být přihlédnuto při definování tarifní politiky například centrálních prvků na národní úrovni, výše poplatků nesmí generovat zisk orgánům, které jsou provozovateli a zároveň jsou zřízeny státem;
- Zákon č. 168/1999 Sb. o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů;



- Zákon č. 22/1997 Sb. o technických požadavcích na výrobky. Dle tohoto zákona organizace provozují Certifikační orgán či provozují zkušební laboratoř pro stanovené výrobky (k 4/2021 nejsou stanoveny požadavky na C-ITS stanice). Posuzování shody je tímto zákonem definováno jako splnění všech specifikovaných požadavků na výrobek, proces nebo službu. Posuzování shody je tedy jakákoliv činnost zabývající se přímým nebo nepřímým určováním, zda byly splněny příslušné požadavky;
- Zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů. Zákon zohledňuje povinnosti definované ve Směrnice Evropského parlamentu a Rady 2010/40/EU ze dne 7. července 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy.
- Zákon č. 12/1997 Sb., o bezpečnosti a plynulosti provozu na pozemních komunikacích;
- Zákon č. 111/1994 Sb. o silniční dopravě, ve znění pozdějších předpisů.

3.1.3.2 Vyhlášky

Vyhlášky, které mohou ovlivňovat ekosystém C-ITS jsou následující:

- Vyhláška č.341/2002 Sb. o schvalování technické způsobilosti a o technických podmínkách provozu vozidel na pozemních komunikacích;
- Vyhláška č.100/2003, kterou se mění Vyhláška MD č.341/2002 podle ustanovení § 15 odst. 1 a násl. Zákona č. 168/1999 Sb., o pojištění odpovědnosti z provozu vozidla je nutné získat platné osvědčení o homologaci pro prvek a platné osvědčení o schválení technické způsobilosti.

3.1.3.3 Usnesení Vlády ČR

Usnesení Vlády ČR, které mohou ovlivňovat ekosystém C-ITS jsou následující:

- Usnesení Vlády ČR č. 590 ze dne 18. května 2005. Tímto usnesením je definován Jednotný systém dopravních informací (JSDI) pro ČR, který je společným projektem Ministerstva dopravy, Ředitelství silnic a dálnic ČR. JSDI je komplexním systémovým prostředím pro sběr, zpracování, sdílení, distribuci a publikaci dopravních informací a dopravních dat o aktuální dopravní situaci a informací o pozemních komunikacích. Hlavním cílem realizace projektu JSDI je informační podpora procesů pro zajištění průjezdnosti a sjízdnosti sítě pozemních komunikací v maximu času a maximu rozsahu území České republiky a zvýšení bezpečnosti a plynulosti provozu prostřednictvím vytvoření spolehlivého, funkčního, efektivního, bezpečného a k životnímu prostředí šetrného systému v silniční dopravě;
- Usnesení Vlády ČR č.35 ze dne 13.ledna 2020: Strategická vize Implementace a rozvoje sítí 5G v České republice – Cesta k digitální ekonomice;
- Usnesení vlády č. 104 ze dne 4. února 2019: Inovační strategie ČR 2019-2030.



3.1.3.4 Další národní strategické dokumenty

Národní strategie v oblasti dopravy navazují na mezinárodní strategie a blíže specifikují řešení v dílčích oblastech. Klíčovými národními strategickými dokumenty jsou Dopravní politika ČR a Dopravní sektorové strategie.

Strategické dokumenty v oblasti telematiky navazují na cíle a vize stanovené ve strategických dokumentech resortu dopravy. Klíčovými dokumenty v oblasti telematiky jsou:

- Akční plán rozvoje inteligentních dopravních systémů a
- Implementační plán rozvoje inteligentních dopravních systémů v ČR
- Strategie ITS s výhledem do roku 2050
- Koncepce rozvoje C-ITS v ČR

3.2 Evropské standardy a normy

Standardy a normy jsou základním prvkem pro zajištění vzájemné interoperability C-ITS zařízení a systémů napříč evropským trhem. Tyto standardy jsou v Evropě vydávány těmito organizacemi:

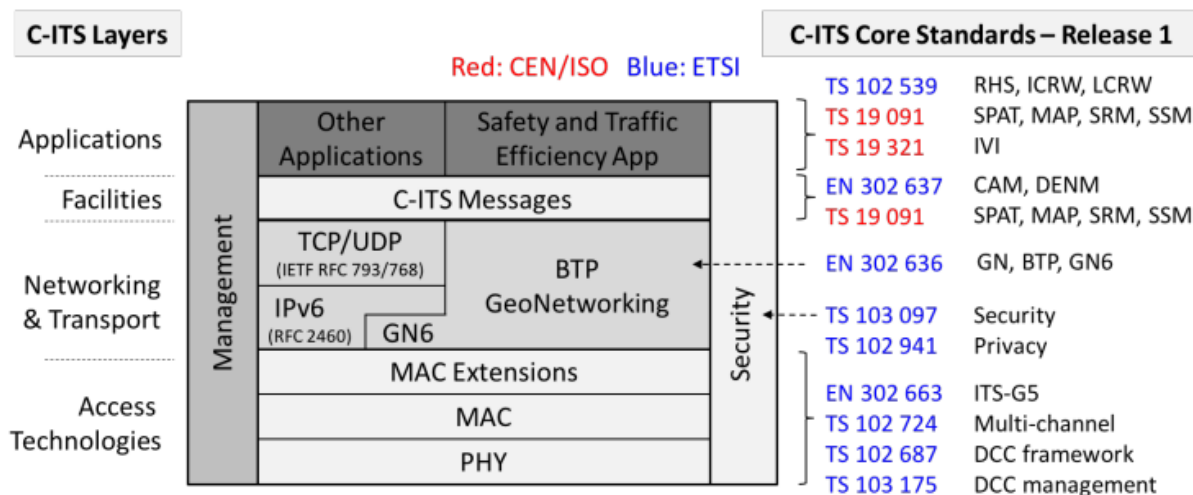
- ETSI – Evropský ústav pro telekomunikační normy (European Telecommunications Standards Institute)
- CEN – Evropský výbor pro normalizaci (Comité Européen de Normalisation)

Mezi další organizace zabývající se standardizací v souvislosti C-ITS jsou:

- ISO – Mezinárodní organizace pro normalizaci (International Organization for standardization)
- IEEE – Institute of Electrical and Electronics Engineers
- SAE – SAE International

C-ITS systémy mohou pro obousměrnou komunikaci mezi vozidly navzájem a mezi vozidly a infrastrukturou využívat různé technologie. Zdaleka nejrozšířenější a v Evropě nejpoužívanější je specifická DSRC technologie operující na frekvenci 5,9 GHz. Toto frekvenční pásmo bylo celosvětově vyhrazeno pro bezpečnostní aplikace v dopravě. V rámci této komunikace je využíváno IEEE standardu 802.11p, který byl v Evropě dále rozpracován standardizační organizací ETSI do podoby ITS-G5. Soubor těchto standardů definuje komunikační architekturu, technické a funkční požadavky na jednotlivé prvky systému včetně zajištění bezpečnosti komunikace v celém systému, podobu přenosového protokolu, atd. Základní SW architektura C-ITS zařízení včetně klíčových norem a standardů pokrývajících jednotlivé úrovně je uvedena na obrázku a v tabulce níže.





Obrázek 10 Architektura C-ITS SW stacku (zdroj: IEEE Communication Magazine, Vol. 53)

Označení	Název
ETSI TR 101 607 V1.2.1 (2020-02)	Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1
ETSI TS 103 301 V1.3.1 (2018-08)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services
ETSI TS 102 687 V1.2.1 (2020-02)	Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part
ETSI EN 302 571 V2.1.1 (2017-02)	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
ETSI TS 102 965 V1.5.1 (2020-01)	Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration
ETSI TS 102 940 v1.3.1 (2018-04)	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI TS 102 941 V1.3.1 (2019-02)	Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
ETSI TS 103 097 v1.4.1 (2020-10)	Intelligent Transport Systems (ITS); Security; Security header and certificate formats

ETSI EN 302 636-4-1 V1.4.1 (2020-01)	Intelligent Transport Systems (ITS); Vehicular Communication; Geonetworking; Part 4 Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality
ETSI EN 302 636-5-1 V2.2.1 (2019-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol
ETSI EN 302 663 V1.3.1 (2020-01)	Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
ETSI TS 103 175 V1.1.1 (2015-06)	Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium
ETSI EN 302 931 V1.1.1 (2011-07)	Vehicular Communications; Geographical Area Definition
ETSI EN 302 637-2 V1.4.1 (2019-04)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
ETSI EN 302 637-3 V1.3.1 (2019-04)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
ETSI EN 302 665 V1.1.1 (2010-09)	Intelligent Transport Systems (ITS); Communications Architecture
ETSI TS 102 724 V1.1.1 (2012-10)	Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band
ETSI TS 102 792 V1.2.1 (2015-06)	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.
ETSI TS 102 894-2 V1.3.1 (2018-08)	Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary
ISO/TS 19321:2020	Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures
ETSI TS 103 248 V1.3.1 (2019-04)	Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)
ETSI TS 102 636-4-2 V1.4.1 (2021-02)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5

ISO/TS 19091:2019	Intelligent transport systems -- Cooperative ITS -- Using V2I and I2V communications for applications related to signalized intersections
ETSI TS 101 539-1 V1.1.1 (2013-08)	Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification
ETSI TR 102 638 V1.1.1 (2009-06)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions

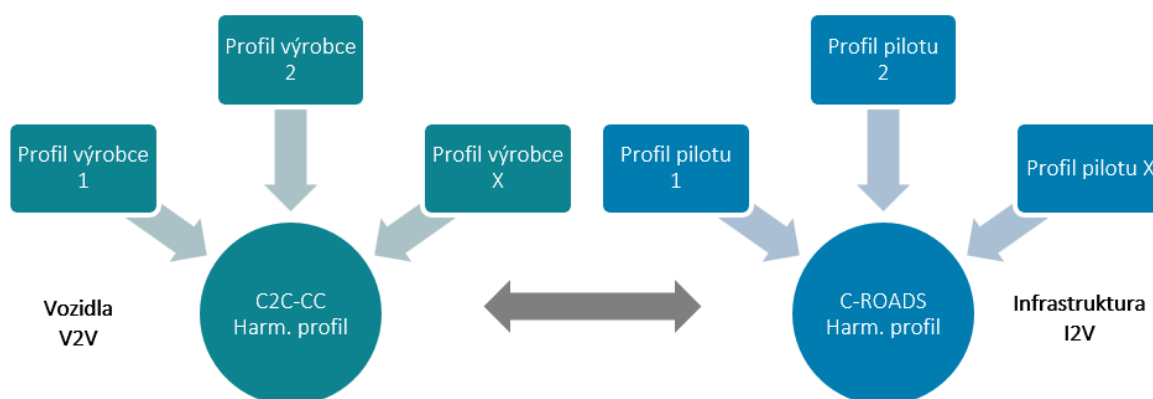
Tabulka 1 Seznam závazných standardů a norem C-ITS

Poznámka: Aktuálně platné verze standardů a norem budou průběžně aktualizovány a doplňovány na stránkách projektu C-ROADS CZ (<https://c-roads.cz/systemy-c-its/technicke-normy-a-standardy/>).

3.3 Harmonizované komunikační profily

Evropské specifikace a normativní dokumenty definují základní podobu C-ITS systému, avšak soubor těchto požadavků stále poskytuje poměrně velký stupeň volnosti při vývoji C-ITS systému. V praxi pak docházelo ke vzájemné komunikační nekompatibilitě C-ITS zařízení v rámci jednotlivých pilotních projektů a rozdílným výkladům jednotlivých C-ITS služeb. Na základě těchto zkušeností byly založeny dvě iniciativy členských států, výrobců vozidel, správců dopravní infrastruktury a dalších partnerů, které analyzovaly dílčí aspekty jednotlivých národních či lokálních specifikací a vytvořily jednotné harmonizované komunikační profily. Harmonizaci komunikačních profilů v oblasti C-ITS se věnují tyto iniciativy:

- C-Roads Platform
- Car-2-Car Communication Consortium



Obrázek 11 Vztah mezi harmonizovanými profily C2C-CC a C-Roads

3.3.1 C-Roads Platform

Mezi klíčové dokumenty vytvořené pan-evropskou platformou C-Roads patří:

- C-ITS Security Requirements and Specifications [3]
- C-ITS Security and Governance [4]
- C-ITS Service and Use Case Definitions [5]
- C-ITS Message Profiles and Parameters [6]
- C-ITS Mobile Roadside ITS G5 System Profile [7]
- C-ITS Roadside ITS G5 System Profile [8]
- C-ITS IP Based Interface Profile [9]

Zároveň platforma C-Roads vydala úvodní zastřešující dokument vysvětlující obsah a způsob využití jednotlivých technických specifikací - Introduction to the C-Roads WG2 Deployment Documentation and Requirements [2].

Aktuálně platné dokumenty vytvořené platformou C-Roads jsou k dispozici na vyžádání na stránce <https://www.c-roads.eu/platform/documents.html>.

Dokumenty vytvořené v rámci platformy C-Roads jsou průběžně aktualizovány a rozšiřovány na základě zkušeností jednotlivých členských států s vývojem a implementací C-ITS. Platforma C-Roads průběžně vydává nová vydání (tzv. „release“) dokumentů uvedených výše. Změny a rozšíření v těchto dokumentech jsou zapracovávány jednotlivými pracovními skupinami (tzv. „Task Forces“) na základě vstupů od jednotlivých členských států. Navržené změny a rozšíření jsou následně schvalovány řídicím výborem (tzv. „Steering Committee“). Pro C-ITS služby specifikované v dokumentech C-Roads platí podmínka předchozí implementace a testování v alespoň jedné členské zemi. V opačném případě je služba specifikována pouze v neveřejných verzích dokumentů, které jsou zařazeny do dalších vydání specifikací až po ověření funkčnosti v reálném prostředí.

3.3.2 Car2Car Communication Consortium

Požadavky vytvořené v rámci konsorcia C2C jsou sdruženy do souboru dokumentů pod názvem Basic System Profile. Tyto dokumenty jsou ke stažení na stránce <https://www.car-2-car.org/documents/basic-system-profile/>.

Harmonizovaný komunikační profil vytvářený konsorciem C2C je stále rozvíjen a aktualizován, kdy každý rok vychází nová vydání (tzv. „release“), které obsahuje nové funkce a služby, opravy chyb. Nové vydání specifikací má být však vždy zpětně kompatibilní. Zásadní změny ve specifikacích jsou schvalovány partnery C2C. K 21.9.2021 je nejnovější vydání specifikací C2C BSP 1.6.0. Opravy chyb, které nemají vliv na zpětnou kompatibilitu systému, jsou vydávány v průběhu roku formou samostatných verzí.

3.4 Národní specifikace

Tato kategorie představuje dokumenty, které specifikují C-ITS systém nad rámec normativních dokumentů a harmonizovaného evropského komunikačního profilu. V rámci těchto dokumentů je



řešena interoperabilita a propojení systému na úrovni České republiky (nikoliv obecná přeshraniční interoperabilita systému). Národní specifikace tak vhodně doplňuje předešlé kategorie a dále snižuje stupeň volnosti při budování systému. Za národní specifikace lze považovat tento dokument (Specifikace systému, Release 2), neboť mimo jiné definuje komunikační rozhraní s národními centrálními prvky, tj.:

- Specifikace rozhraní s Integrovanou platformou (viz kap. č. 4.5.3)
- Specifikace rozhraní s PKI (viz kap. č. 4.5.7)

3.5 Specifické požadavky

Mimo závazné standardy a normy je v rámci implementace nutné dodržovat i požadavky, které nutně nesouvisí se zajištěním interoperability C-ITS systému, ale představují převážně funkční a technické požadavky na provedení fyzické instalace zařízení na infrastrukturu nebo do vozidel. Tyto požadavky se mohou výrazně lišit na základě prostředí, ve kterém jsou instalace prováděny. Může se tak jednat o interní předpisy správce infrastruktury (např. Požadavky na provedení a kvalitu PPK ŘSD), specifické požadavky výrobce vozidla či typu vozidel (např. požadavky Drážního úřadu). Interní specifické požadavky na C-ITS systémy v rámci jednotlivých organizací musejí být vždy v souladu s požadavky specifikací nadřazených (viz kapitoly výše).

4 Ekosystém C-ITS

V rámci projektu C-ROADS CZ byla definována společná architektura celého ekosystému, podle které probíhala následná implementace C-ITS systémů a služeb na jednotlivé pilotní lokality. Tato navržená architektura se v průběhu projektu osvědčila jako funkční, a byla tak začleněna také do národní Koncepce rozvoje C-ITS v ČR [26] zpracované ŘSD ČR.

Z technického pohledu se C-ITS systém se skládá ze tří základních vrstev, které tvoří základ systému. Jedná se o:

- **Vozidlové C-ITS jednotky** – OBU (On board unit), jedná se o C-ITS stanici ve vozidle;
- **C-ITS jednotky umístěné na infrastruktuře** – RSU (Road side unit), jedná se o C-ITS stanici na infrastruktuře;
- **Centrální C-ITS stanice** – C-ITS Back Office.

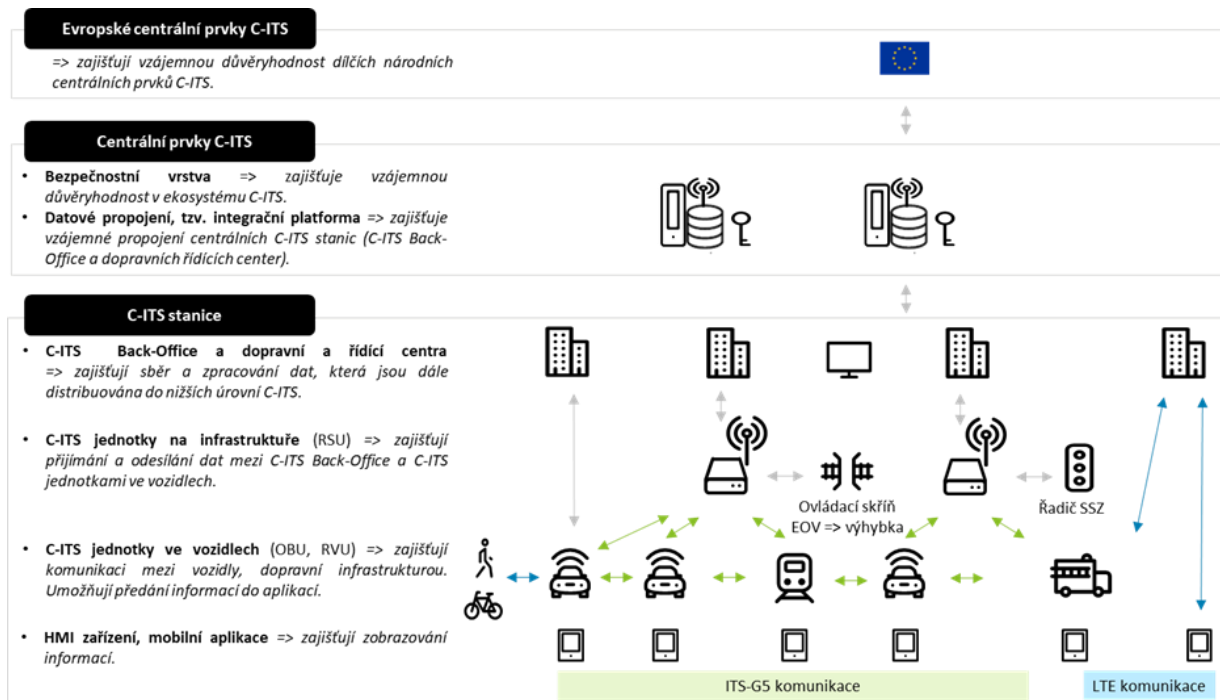
Tyto základní prvky byly následně na základě zkušenosti z pilotních projektů rozšířeny o další vrstvy:

- **Centrální prvky** (Integrační platforma, PKI – bezpečnostní vrstva) zajišťující výměnu C-ITS zpráv a také spolehlivost a bezpečnost systému;
- **Mobilní aplikace**, které představuje skupinu aplikací pro mobilní telefony a tablety, které jsou schopné interpretovat přijaté C-ITS zprávy.

Kromě těchto komponent jsou nezbytné i informační zdroje zastoupené například dopravními a řídicími centry.

Uspořádání těchto prvků představuje fyzickou a komunikační architekturu systému, která je zobrazena na schématu níže.





Obrázek 12 Popis komponent ekosystému C-ITS (zdroj: Koncepce rozvoje C-ITS v ČR)

4.1 Centrální prvky C-ITS

Centrální prvky C-ITS jsou tvořeny prvky na nadnárodní (evropské) a na národní úrovni v ČR.

Centrální evropské komponenty jsou budovány Evropskou komisí pod společným označením European Union C-ITS Security Credential Management System (EU CCMS). Jeho součástí jsou následující komponenty:

- Trust List Manager (TLM)
- European Certificate Trust List (ECTL)
- C-ITS Point of Contact (CPOC)

Tyto komponenty slouží k zajištění pan-evropské interoperability a zajištění vzájemné důvěry mezi různými PKI systémy. Na konci roku 2021 bylo k dispozici testovací prostředí těchto komponent (tzv. úroveň L0) a zároveň byla ustanovena expertní skupina pro vytvoření podmínky pro provoz přechodného produkčního prostředí těchto komponent – tzv. úroveň L1. Cílový stav je tzv. úroveň L2, která už bude plně respektovat podmínky stanovené v dokumentech Evropské komise – C-ITS Certificate Policy [24] a C-ITS Security Policy [25].

Na národní úrovni centrální C-ITS prvky tvoří:

- Bezpečnostní vrstva
- Integrační platforma



Pro potřeby zajištění provozu centrálních prvků C-ITS po skončení projektu C-ROADS CZ vypsalo ŘSD ČR veřejnou zakázku na poskytování služby. K 27.7.2021 byla uzavřena smlouva s novým poskytovatelem centrálních prvků C-ITS a k 17. 9. 2021 byla služba Integrovaná platformy a bezpečnostní vrstvy spuštěna do plného provozu a je připravena pro registraci C-ITS stanic a centrálních prvků. Provozovatel centrálních prvků stanoví technické, funkční a procesní požadavky pro připojení dalších C-ITS stanic. Požadavky, jejichž splnění bude podmínkou pro připojení k platformě, budou definovány v samostatném dokumentu, který bude zpracován do konce roku 2021. Tímto opatřením bude zajištěna stejná úroveň kvality a důvěryhodnosti C-ITS zpráv, které jsou prostřednictvím Integrovaná Platformy sdíleny mezi koncovými C-ITS jednotkami jednotlivých provozovatelů (ŘSD, BKOM, DPMB aj.) a které jsou díky systému PKI vzájemně důvěryhodné.

4.1.1 Bezpečnostní vrstva – PKI

Tato část systému zajišťuje bezpečnost a důvěryhodnost všech C-ITS částí systému. Technologicky je tato část systému vystavěna na principech distribuce veřejných klíčů („Public Key Infrastructure“) a stará se o správu a výměnu veřejných klíčů, čímž je vytvářen ekosystém vzájemné důvěry mezi jednotlivými prvky systému. Další informace k tomuto tématu jsou uvedeny v kap. č. 5.

4.1.2 Integrovaná platforma

Integrovaná platforma zajišťuje vzájemné propojení C-ITS Back Offices jednotlivých subjektů (např. správců dopravní infrastruktury, správců dopravní infrastruktury ve městech, dopravních podniků a dalších), případně i mezi dopravními centry (např. NDIC). Integrovaná platforma umožňuje propojení různorodých systémů tak, aby byla zabezpečena spolehlivá výměna dat mezi těmito systémy. Komunikace probíhá zvoleným protokolem, při kterém je zachován specifický formát C-ITS zpráv.

Komunikační rozhraní mezi Integrovanou platformou a jednotlivými C-ITS BO je popsáno v kap. č. 4.5.3.

4.2 Centrální C-ITS stanice a informační zdroje

Tato kategorie se v kontextu České republiky dělí na dvě části:

- C-ITS Back Office
- Informační zdroje

4.2.1 C-ITS Back Office

C-ITS Back Office plní funkce:

- Koncentruje a zpracovává většinu dat
- Distribuuje data do prvků na nižších úrovních systému (RSU, OBU, mobilní aplikace) dle jasných pravidel
- Zajišťuje komunikaci s dalšími externími systémy (např. informační zdroji, Integrovanou platformou).



- Poskytuje základ pro vizualizace a mapy
- Zajišťuje manuální vytváření událostí (resp. C-ITS zpráv včetně jejich podpisu)
- Automaticky generuje C-ITS zprávy na základě dat z externích systémů
- Umožňuje uživatelský management, archivaci a další související funkce.

Základní doporučené technické a funkční požadavky na C-ITS BO je možné popsat pomocí jednotné architektury zaručující otevřenost a rozšiřitelnost systému pro budoucí C-ITS služby, přenosové cesty, popř. pro geografické pokrytí ITS službami tak, aby do něj snadno mohly být zapojeny nové moduly bez nutných změn v architektuře systému.

Závažné technické a funkční požadavky na C-ITS BO jsou dány obecnými požadavky na tvorbu C-ITS zpráv (viz kap. č. 3) a požadavky na jednotlivá rozhraní mezi C-ITS BO a dalšími prvky systému (viz kap. č. 4.5).

4.2.2 Informační zdroje

Tato kategorie představuje ucelené systémy, které nemusí plnit funkce primárně sloužící pro C-ITS systémy, ale mohou představovat důležité vstupní informace do systému C-ITS. Systém C-ITS může na druhé straně poskytovat hodnotné informace do těchto systémů.

4.2.2.1 JSDI/NDIC

Jednotný systém dopravních informací (dále také „JSDI“) je komplexní systémové prostředí pro sběr, zpracování, sdílení, distribuci a publikování dopravních informací a dopravních dat o aktuální dopravní situaci a informací o pozemních komunikacích, jejich součástech a příslušenství (centrální evidence pozemních komunikací) od orgánů, organizací a institucí veřejné správy a od dalších veřejných i privátních subjektů.

Národní dopravní informační centrum (dále také „NDIC“) je centrálním technickým, technologickým, provozním i organizačním pracovištěm JSDI. Jde o operační pracoviště, které 24 hodin denně 7 dní v týdnu zajišťuje sběr, zpracování, vyhodnocování, ověřování a autorizaci dopravních informací a dopravních dat. Jádrem NDIC je telematická platforma založená na modelu dopravy, která poskytuje podklady pro operátorský dohled a koordinované řízení a ovlivnění aktuálního provozu.

NDIC předává do C-ITS systému množství dopravních událostí, které byly identifikovány a validovány různými systémy v rámci JSDI. Integrační platforma zajišťuje konverzi událostí z formátu DATEX II do formátu C-ITS zpráv a umožňuje jejich odběr napojeným subjektům (C-ITS Back Offices).

4.2.2.2 Městské dopravní a řídicí systémy

Z pohledu C-ITS systémů představuje tato kategorie centralizovaná dopravní centra, kde jsou agregována a zpracovávána dopravní data ze zájmového území, která mohou být dále využita pro vytváření C-ITS zpráv v C-ITS Back Office a zároveň mohou konzumovat i dopravní data získávána



prostřednictvím C-ITS technologie ve vozidlech a na infrastruktuře. Představitelem této skupiny informačních zdrojů jsou dopravní informační centra (např. v Praze, Brně, či jiných).

4.3 C-ITS stanice

C-ITS stanice se v kontextu České republiky dále dělí na následující typy:

- C-ITS jednotky na infrastruktuře
- C-ITS jednotky ve vozidlech a vozících
- Mobilní aplikace

4.3.1 C-ITS jednotky na infrastruktuře

Jednotka RSU (Roadside Unit) je prvkem zajišťujícím přímou komunikaci s vozidlovými jednotkami a také s centrálními prvky (C-ITS Back Office). Jednotka RSU se instaluje na stávající nebo i na novou technicko-technologickou infrastrukturu umístěnou v okolí dopravních staveb (výložníky SSZ, sloupy veřejného osvětlení, sloupy trakčního vedení aj). RSU jednotky na těchto lokalitách řidičům předávají důležité informace o dopravních událostech v jejich okolí a zároveň od vozidel přijímají data, která jsou ještě na úrovni RSU agregována, předzpracována a následně odeslána do C-ITS Back Office.

Jednotka RSU plní následující funkce:

- Přijímá a odesílá data z/do C-ITS Back Office (přes pevné datové sítě, pokud je jejich využití možné, alternativně lze jako záložní řešení využít i datové sítě mobilních operátorů)
- Generuje vlastní C-ITS zprávy v rámci definovaných Use Cases
- Přijímá a odesílá data z/do vozidel pomocí standardu ITS-G5
- Zpracovává data přímo v jednotce RSU, popř. je ukládá předtím, než jsou odesílány dále

Tyto jednotky mohou být zároveň napojeny na další zařízení na infrastruktuře (řadič SSZ, ovládací skříň EOV, detektory), díky čemuž mohou automaticky generovat určitý typ zpráv. Tímto propojením vznikne možnost využít C-ITS technologii k zajištění preference vybraného typu vozidel na křižovatce, sdílení aktuálního signálu SSZ pro jednotlivé směry či zažádání tramvaje o změnu polohy výhybky.

Funkční a technické specifikace C-ITS jednotek na infrastruktuře jsou definovány především standardy a normami (viz kap. č. Chyba! Nenalezen zdroj odkazů.) a evropskými harmonizačními dokumenty, které byly vytvořeny platformou C-Roads, tj. zejména těmito dokumenty:

- Roadside ITS G5 System Profile [7]
- C-ITS Message Profiles [6]
- C-ITS Service and Use Case Definitions [5]



Další specifikace C-ITS jednotek na infrastrukturu se mohou výrazně lišit na základě prostředí, ve kterém jsou instalace prováděny.

4.3.2 C-ITS jednotky ve vozidlech

Jedná se o C-ITS jednotky instalované do vozidel (osobní vozidla, nákladní vozidla, tramvaje, autobusy apod.). Tyto jednotky umožňují příjem a generování C-ITS zpráv, které jsou následně rozesílány dalším vozidlům, RSU jednotkám nebo centrálním C-ITS stanicím.

C-ITS jednotky ve vozidlech jsou součástí C-ITS systémů, které zajišťují komunikaci:

- Mezi vozidly a dopravní infrastrukturou v rámci standardu ITS-G5 na dedikovaných frekvencích v pásmu 5,9 GHz. C-ITS systémy umožňují vysokorychlostní předávání informací zejména pro definované bezpečnostní aplikace a aplikace zaměřené na řízení a informování v oblasti dopravy.
- S centrální stanicí systému, tzn. C-ITS Back Office prostřednictvím datových sítí mobilních operátorů (např. LTE, 5G).

Tyto jednotky mohou být napojeny na vozidlové systémy nebo přídavné senzory a vyčítat tak například potřebná data pro účely automatických generování dalších C-ITS služeb. Jednotka je pro tyto účely osazena do vozidla již z výroby nebo může být instalována i dodatečně (tzv. „retrofit“). Jednotka může být dále propojena s HMI zařízením (zde hovoříme o tabletu, mobilním telefonu nebo displeji přímo ve vozidle), které musí být vybaveno vhodným SW nástrojem pro komunikaci s jednotkou, pro účely zobrazování C-ITS zpráv řidiči.

V některých případech se C-ITS jednotky ve vozidlech ještě rozlišují do dvou kategorií, tj.:

- **OBU (On-board unit)**
Tyto jednotky jsou umístěné přímo v jednotlivých vozidlech koncových uživatelů (řidičů) a zajišťují komunikaci s vybavením na infrastrukturu a ostatními C-ITS jednotkami v okolních vozidlech (viz kap. č. 4.5.1). Nad rámec přímé komunikace mohou přijímat C-ITS zprávy z C-ITS Back Office, ke kterému jsou registrovány.
- **RVU (Road-vehicle Unit)**
Tyto jednotky představují „hybrid“ mezi stacionárními jednotkami na infrastrukturu RSU a OBU, neboť mohou sloužit k zajištění přímé komunikace s vybavením na infrastrukturu a s ostatními vozidlovými C-ITS jednotkami v okolí jako jednotky OBU, ale zároveň se mohou stát samy vybavením na infrastrukturu a částečně plnit funkci RSU jednotek a zajišťovat tak diseminaci C-ITS zpráv ve svém okolí (viz kap. č. 4.5.1). V rámci projektu C-ROADS CZ byly jednotky RVU například použity v mobilních vozících či vozidlech údržby správce komunikací, a zahušťují tak síť pokrytí jednotkami RSU.



Z pohledu HW požadavků se OBU a RVU jednotky neliší a rozdíl je pouze v SW nastavení dané vozidlové C-ITS jednotky. Z toho důvodu bude níže v textu používán souhrnný název vozidlové C-ITS jednotky nebo OBU.

Funkční a technické specifikace C-ITS jednotek ve vozidle jsou definovány především standardy a normami (viz kap. č. Chyba! Nenalezen zdroj odkazů.) a evropskými harmonizačními dokumenty, které byly vytvořeny platformou C-ROADS a Car-2-Car, tj. zejména těmito dokumenty:

- **Mobile Roadside ITS G5 System Profile [7] – pro retrofit instalace C-ITS**
- **Basic System Profile, C-ITS Message Profiles [13] – instalace C-ITS již ve výrobě**
- **C-ITS Message Profiles [6]**
- **C-ITS Service and Use Case Definitions [5]**

Další specifikace C-ITS jednotek na infrastrukturu se mohou výrazně lišit na základě prostředí, ve kterém jsou instalace prováděny. Může se tak jednat o interní předpisy správce vozového parku, specifické požadavky výrobce vozidla či typu vozidel (např. požadavky Drážního úřadu). Před samotnou instalací je proto vždy vhodné vytvořit instalační manuál, který je před samotnou instalací schválen správcem daného subjektu.

4.3.3 Mobilní aplikace

Mobilní aplikace (instalovaná např. v mobilním telefonu, tabletu) umožňují přijímat C-ITS zprávy z C-ITS Back Office, ke kterému jsou registrovány prostřednictvím datových sítí mobilních operátorů (viz kap. č. 4.5.2) bez nutnosti propojení s C-ITS jednotkou ve vozidle. Nemohou však přijímat napřímo zprávy generované jednotkami OBU a RSU prostřednictvím ITS-G5 (viz kap. č. 4.5.1). Mobilní aplikace může být pouze pasivní, tj. pouze přijímá C-ITS zprávy, nebo může být plnohodnotným aktorem, tj. C-ITS zprávy přijímá i generuje. V druhém případě se pak na takovou aplikaci vztahují stejná pravidla a požadavky jako pro „plnohodnotnou“ OBU jednotku (viz kap. č. 4.3.2).

Tato zařízení představují alternativu k vozidlovým C-ITS jednotkám po dobu nízké penetrace vybavených vozidel C-ITS technologií. Použití těchto zařízení je limitováno latencí datového přenosu C-ITS zpráv a také výkonovými parametry HW zařízení – tabletu či mobilního telefonu. Není to vhodná varianta pro poskytování tzv. „time-critical“ C-ITS služeb (např. prudká brzdění). Potenciál pro rozšíření využití mobilních aplikací pro větší paletu služeb vč. „time-critical“ služeb představuje rozšíření pokrytí datových sítí 5G a s tím spojené zvýšení kapacity a snížení latence datové sítě.



4.4 Přenosové komunikační technologie

Z pohledu C-ITS systémů lze přenosové komunikační technologie rozdělit do těchto kategorií:

- Komunikace na krátkou vzdálenost
 - ITS-G5
 - LTE-V2X / PC5 Sidelink
- Komunikace na delší vzdálenost
 - Stávající datové sítě (3G, LTE, 4G)
 - Nové datové sítě 5G

V případě kombinace komunikačních technologií, tzn. současného využití komunikace na krátkou vzdálenost a komunikace pro delší vzdálenost, pro přenos C-ITS zpráv je systém označován jako „hybridní“. V rámci projektu C-Roads Czech Republic bylo provozováno právě „hybridní“ řešení, kdy byla kombinována komunikace prostřednictvím ITS-G5 a stávajících datových sítí (3G, 4G). Během krátkodobých testů byla zároveň ověřena komunikace prostřednictvím LTE-V2X.

4.4.1 ITS-G5

ITS-G5 je evropská sada protokolů pro komunikaci vozidlo-vozdílo (V2V) a vozidlo-infrastruktura (V2I) založená na standardu IEEE 802.11 (používaný také pro WiFi) a jeho rozšíření 802.11p, který byl upraven a optimalizován pro potřeby automobilového prostředí. V Evropě byl standard IEEE 802.11p přetvořen do podoby ITS-G5 organizací European Telecommunications Standards Institute (ETSI), proto je někdy označován také jako ETSI ITS-G5. V USA byl tento standard rozpracován do podoby WAVE (Wireless Access in Vehicular Environment). ITS-G5 byl definován v Evropě v roce 2004 a od té doby proběhlo mnoho standardizačních procesů a pilotních testů, díky čemuž je nyní tato technologie považována za ověřenou, spolehlivou a vhodnou pro nasazení do běžného provozu. Tomu odpovídá i trh, na kterém se objevují certifikované produkty splňující standardy a normy ETSI a ISO/CEN. Další informace k standardizaci ITS-G5 jsou uvedeny kap. č. 3.2.

ITS-G5 umožňuje přímou vzájemnou 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 Dedicated short-range communications technologie (DSRC) technologie operující na frekvenci 5,9 GHz. Frekvence 5,9 GHz funguje v pásmu, které je vyhrazeno pouze pro dopravní služby, díky čemuž je možné zaručit určitou kvalitu a dostupnost služeb. Zároveň je nespornou výhodou využívání ITS-G5 absence jakýchkoliv poplatků za využívání tohoto pásma. V současné době představuje ITS-G5 zdaleka nejpoužívanější komunikační technologii pro projekty v oblasti kooperativních systémů v Evropě.

Vyhrazená frekvence 5,9 GHz pro technologii ITS-G5 je nyní v Evropě rozdělena na následující pásma:

- ITS-G5B 5855 – 5875 MHz – ITS aplikace, které nejsou bezpečnostní
- ITS-G5A 5875 – 5905 MHz – bezpečnostní ITS aplikace
- ITS-G5D 5905 – 5925 MHz – budoucí ITS aplikace



ITS-G5 technologie není svázána s poskytovatelem služeb mobilního operátora, ale je definována samotným zařízením, jehož provozovatel může být správce komunikací, poskytovatel služeb, výrobci vozidel aj.

Evropské normy (ETSI, ISO/CEN) týkající se ITS-G5 definují frekvenční rozsahy a protokoly, které mají být použity pro komunikaci mezi C-ITS jednotkami a definují základní architekturu systému. Zároveň definují metody a nástroje pro zajištění koexistence se systémy pracujícími v blízkém komunikačním spektru, např. rušení systémů pro výběr mytného v rozsahu 5,8 GHz (CEN-DSRC) a decentralizovaný způsob řízení přetížení komunikačního spektra (Decentralized congestion control – DCC), který řídí vysílání jednotlivých zařízení, aby nedošlo ke kongesci zpráv při velkém počtu komunikujících jednotek.

4.4.2 Mobilní datové sítě

Kromě komunikace krátkého dosahu se pro přenos zpráv v rámci C-ITS služeb využívají také stávající datové sítě mobilních operátorů. Jedná se především o sítě čtvrté generace (definované v 3GPP Release 8 a dále), popř. jsou pro některé C-ITS služby použitelné i sítě 3G. Starší generace datových sítí už nejsou z důvodu svých výkonových parametrů pro C-ITS služby vhodné. S použitím těchto komunikačních technologií je svázáno zasmluvnění datových služeb s mobilním operátorem při zakoupení fyzického zařízení na infrastrukturu nebo do vozidla. Poskytovatel C-ITS přes mobilní datové sítě tak musí zajistit funkčnost zařízení a specifikaci rozhraní a tvorbu kvalitních dat, ale zodpovědnost za přenos samotné datové zprávy (komunikační spojení) převezme mobilní operátor.

4.4.3 Hybridní komunikace

V souvislosti s výše uvedenými informacemi a stanoviskem členských států projektu C-Roads se jeví jako nejvhodnější řešení na území ČR nadále podporovat využití tzv. hybridního C-ITS systému, kdy jsou C-ITS zprávy na krátkou vzdálenost vysílány primárně prostřednictvím technologie ITS-G5 a zároveň jsou zprávy vysílány prostřednictvím mobilních datových sítí. Právě hybridní řešení, které kombinuje výhody ITS-G5 pro komunikaci zařízení na krátkou vzdálenost (kde je zapotřebí zajistit maximální interoperabilitu a minimální zpoždění zprávy) a stávajících datových služeb pro komunikaci na delší vzdálenosti, je v posledních letech implementováno na území všech členských zemí projektu C-Roads. Kombinace ITS-G5 a stávajících datových sítí pro hybridní distribuci C-ITS zpráv je označena v Evropské strategii pro C-ITS (COM (2016) 766) [15] jako nejvhodnější varianta, stejně tak je tomu v národní Konceptu rozvoje C-ITS [26].

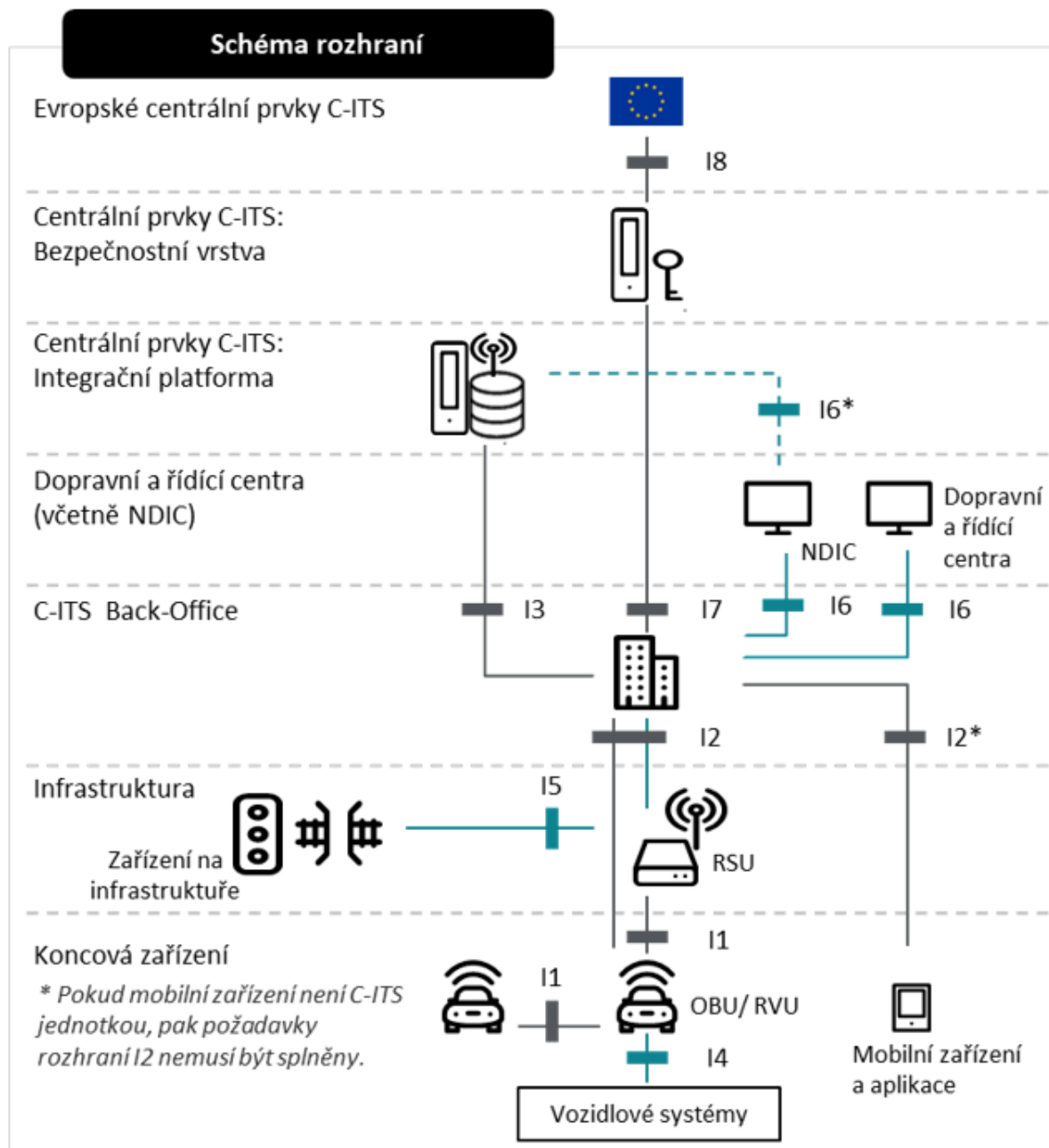
4.5 Komunikační rozhraní mezi prvky systému

Mezi jednotlivými prvky C-ITS systému existují rozhraní, která mají své specifické požadavky. Některá rozhraní jsou jasně definována mezinárodními standardy, jiná byla definována na národní úrovni, neboť specifické požadavky v jednotlivých zemích nepředstavují pro zajištění mezinárodní interoperability žádnou překážku. V každém případě však musí být zachována maximální otevřenost celého systému.



Co se týče fyzické přenosové vrstvy, rozhraní v rámci C-ITS systému jsou v zásadě dvojího typu – realizovaná prostřednictvím pevného spojení (ethernet s využitím optických či metalických kabelů) a dále bezdrátová rozhraní využívající komunikaci dlouhého či krátkého dosahu. V C-ITS systému byla definována tato rozhraní:

- Rozhraní I1: OBU ↔ OBU / RSU. Detailní popis rozhraní je uveden v kapitole 4.5.1
- Rozhraní I2: C-ITS Back Office ↔ C-ITS zařízení (OBU, APP). Detailně je toto rozhraní popsáno v kapitole 4.5.2
- Rozhraní I3: C-ITS Back Office ↔ Integrovaná platforma. Detailně je toto rozhraní popsáno v kapitole 4.5.3
- Rozhraní I4: OBU ↔ vozidlové systémy. Detailně je toto rozhraní popsáno v kapitole 4.5.4
- Rozhraní I5: RSU ↔ další zařízení na infrastruktuře. Detailně je toto rozhraní popsáno v kapitole 4.5.5
- Rozhraní I6: C-ITS prvky ↔ Další informační zdroje. Detailně je toto rozhraní popsáno v kapitole 4.5.6
- Rozhraní I7: C-ITS Back Office ↔ bezpečnostní vrstva PKI. Detailně je toto rozhraní popsáno v kapitole 4.5.7
- Rozhraní I8: Evropské centrální prvky ↔ bezpečnostní vrstva PKI. Detailně je toto rozhraní popsáno v kapitole 4.5.8



Obrázek 13 Rozhraní systému v rámci C-ITS ekosystému (zdroj: Koncepce rozvoje C-ITS v ČR)

4.5.1 Rozhraní I1: vozidlové jednotky ↔ jednotky na infrastruktuře / vozidlové 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 (až 1000 m).

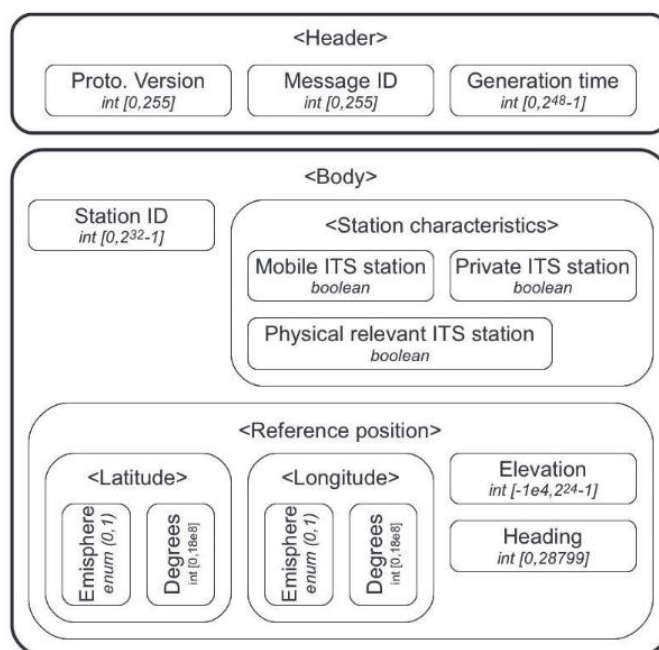
Výhodou této technologie je její rychlost a spolehlivost, přičemž výměna informací může probíhat až desetkrát za vteřinu.

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.

V rámci C-ITS ekosystému jsou generovány a posílány, tyto specifické zprávy:

- **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. CAM bývají často označovány jako „Here I am“ zprávy. Struktura zprávy CAM je znázorněna na následujícím obrázku.



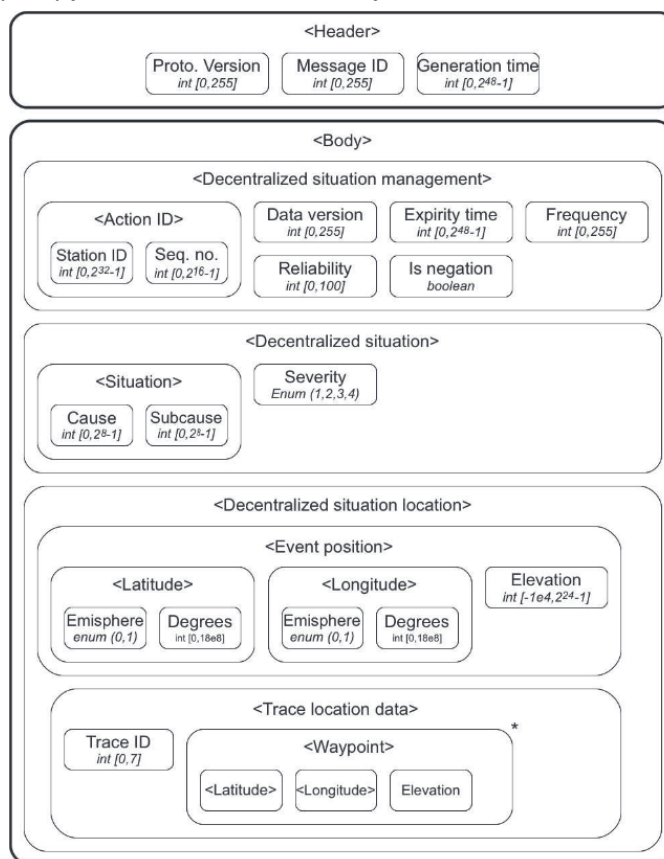
Obrázek 14 Struktura zprávy CAM (zdroj: ETSI TS 102 637-2)

Zprávy CAM jsou mimo jiné využívány pro výpočty dojezdových dob, zdržení, průměrných rychlostí apod. v rámci služby Probe vehicle data. Vždy první CAM zpráva, kterou RSU jednotka obdrží od konkrétní OBU jednotky, je zároveň přeposlána do C-ITS Back Office. Všechny další obdržené CAM zprávy jsou zpracovávány na úrovni RSU jednotky, kde se data agregují dle virtuálních detektorů. Do C-ITS serveru už jsou následně odesílána agregovaná data o provozu v oblasti dosahu příslušné RSU jednotky. 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.

- **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, práce na silnici, kluzká vozovka, jízda v protisměru či jiný typ překážky. Zpráva může být generována v C-ITS Back Office, popř. přímo v OBU/RSU jednotce. RSU jednotky zprávy DENM z C-ITS BO pouze přeposílají do vozidel ve svém dosahu či naopak do C-ITS Back Office dle typu události. Struktura DENM zprávy je znázorněna na následujícím obrázku.

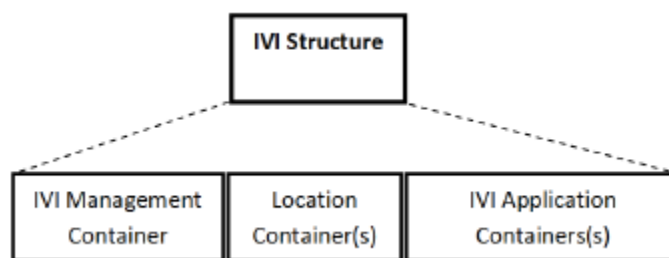


Obrázek 15 Struktura zprávy DENM (zdroj: ETSI TS 102 637-3)

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 ITS jednotka vyšle speciální DENM zprávu, která zruší platnost dotyčné události. Specifikace zprávy DENM je detailně popsána v předpisu 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.

- **In-Vehicle Information (IVIM)**

Zprávy IVIM obecně slouží primárně pro přenos informací o statických a dynamických dopravních symbolech, např. dopravní symboly na portálech liniového řízení dopravy (LŘD) a zařízení pro provozní informace (ZPI), do vozidla. IVIM zpráva je generována přímo v C-ITS Back Office a je následně odeslána do příslušné RSU jednotky či přímo do vozidel v blízkosti daných portálů. V některých případech mohou být IVIM zprávy generovány přímo v RSU. Struktura IVIM zprávy je znázorněna na následujícím obrázku.



Obrázek 16 Struktura zprávy IVIM (zdroj: ISI/TS 19321)

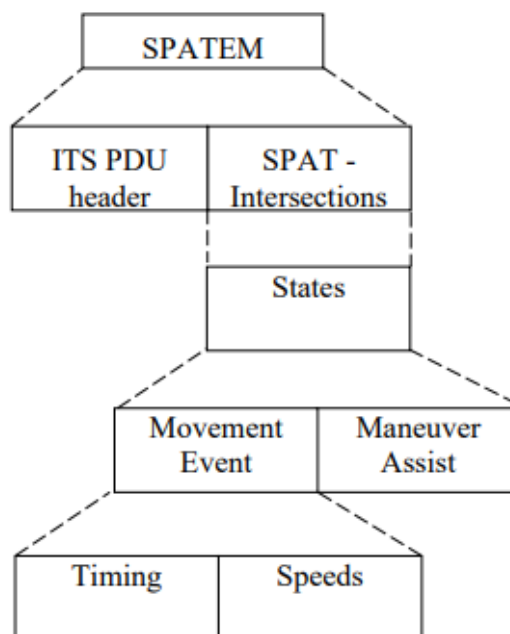
IVIM zpráva neslouží pouze pro přenos zobrazovaných dopravních symbolů, ale také doplňkových textů (portály ZPI). Získané informace jsou následně HMI zařízením ve vozidle vhodně prezentovány řidiči dle knihovny dopravních symbolů a typického rozložení dopravních značení na portálech. Zpráva IVIM je periodicky vysílána až do vypršení doby její přednastavené platnosti, nebo do doby, než je poslána speciální IVIM zpráva, která zruší platnost daných vysílaných dopravních informací. Specifikace IVIM zprávy je detailně popsána v normě ISI/TS 19321:2015 Intelligent transport systems – Cooperative ITS – Dictionary of in-vehicle information (IVI) data structure. Pro kódování jednotlivých dopravních symbolů je primárně použita knihovna definována v normě ISO/TS 14823:2008 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.

- **Signal Phase and Timing Message (SPATEM)**

Zprávy SPATEM slouží k poskytování informací o signálním cyklu světelného signalizačního zařízení (SSZ) na křižovatkách. Tento cyklus určuje pořadí a délku jednotlivých signálních dob. SPATEM je generována v jednotce RSU v blízkosti SSZ na základě informací z dopravního řadiče. Jedna tato zpráva může obsahovat informace o signálním cyklu jedné nebo o více křižovatek zároveň. Po příjmu zprávy SPATEM vozidlovou jednotkou OBU je tato zpráva zpracovávána dohromady se zprávou MAPEM (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 a varovat před průjezdem křižovatkou na signál „stůj“.

Zprávy SPATEM jsou standardizovány dokumentem SAE J2735 Dedicated Short Range

Communications (DSRC) Message Set Dictionary a ISO/TS 19091:2017 Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections.

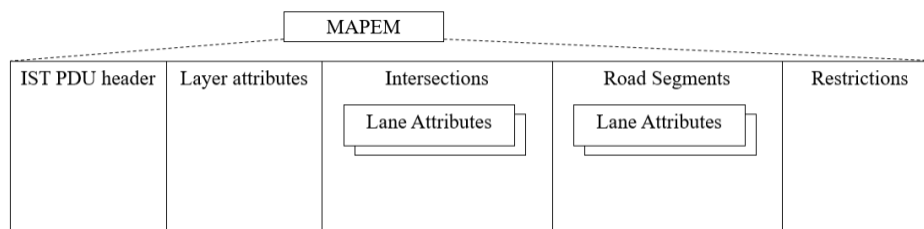


Obrázek 17 Struktura zprávy SPATEM (zdroj: ISO/TS 19091)

- **MAP (topology) Extended Message (MAPEM)**

Zprávy MAPEM slouží k poskytování informací o topologii a geometrii křižovatkových úseků či komplikovaných silničních úseků z jednotek RSU do vozidel nebo do mobilních zařízení. Jedna zpráva MAPEM může obsahovat informace o geometrii jedné, ale i více křižovatek. Po příjmu zprávy MAPEM vozidlovou jednotkou OBU je tato zpráva zpracovávána dohromady se zprávou SPATEM, čímž je stanoven stav světelné signalizace pro každý segment křižovatky (jednotlivé jízdní pruhy).

- Specifikace zprávy MAPEM je popsána v dokumentu ISO/TS 19091:2017 Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections.



Obrázek 18 Struktura zprávy MAPEM (zdroj: ISO/TS 19091)

- **Signal Request Extended Message (SREM)**

SREM zprávy se používají pro odeslání požadavku na preferenční jízdu z vozidla MHD / IZS (popř. další definované skupiny vozidel) směrem k RSU, které připojeno k řadiči SSZ (případně k ovládací skříni EOVS). Případně může být tato zpráva použita pro aktualizaci požadavku. Oproti výše zmiňovaným C-ITS zprávám je SREM adresná a obsahuje číslo křižovatky, ke které se vztahuje požadavek na preferenci. SREM zprávy mohou být zároveň použity pro vyslání požadavku na změnu polohy výhybky.

Specifikace zprávy SREM je definována ve standardu ETSI TS 103 301 Facilities layer protocols and communication requirements for infrastructure services. Tento dokument se dále odkazuje na dokument ISO/TS 19091 Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections a SAE J2735.

- **Signal Status Extended Message (SSEM)**

SSEM zprávy jsou vysílány jako odpověď na příchozí zprávy SRM a obsahují informaci o stavu vyřízení požadavku obsaženém v SREM. Tyto zprávy jsou vysílány vždy RSU jednotkami a podobně jako zprávy SRM jsou SSM adresné.

Specifikace zprávy SSEM je specifikována ve standardu ETSI TS 103 301 Facilities layer protocols and communication requirements for infrastructure services. Tento dokument se dále odkazuje na dokument ISO/TS 19091 Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections a SAE J2735.

- **Další**

V souvislosti s vývojem a testováním nových služeb jsou postupně definovány nové typy zpráv, na jejichž standardizaci se nyní pracuje. Mezi tyto zprávy mohou patřit např.:

- MCM - Maneuver coordination message
- CPM - Collective Perception Message
- RTCMEM - Radio Technical Commission for Maritime services Extended Message
- VAM - Dedicated VRUs awareness

C-ITS zprávy této kategorie v době zpracování tohoto dokumentu ještě nejsou standardizovány.

4.5.2 Rozhraní I2: C-ITS Back Office ↔ C-ITS zařízení

Komunikace mezi C-ITS Back Office a C-ITS jednotkou / mobilní aplikací může být realizována do určité míry proprietárně na základě potřeb a požadavků jednotlivých poskytovatelů C-ITS služeb a správců C-ITS infrastruktury, musí však splňovat obecné požadavky C-ITS systému. Tato volnost se vztahuje zejména na charakter fyzické přenosové vrstvy – v závislosti na dostupnosti komunikační infrastruktury



a na charakteru poskytovaných služeb může být toto rozhraní realizováno jak přes pevné sítě (např. optické kabely na dálnicích), tak přes sítě mobilních operátorů (LTE, 5G).

Co se týče samotného obsahu, komunikaci v rámci rozhraní I2 lze rozdělit do dvou kategorií, tj.:

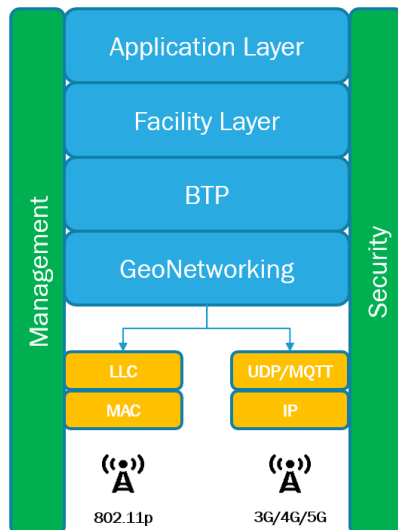
- C-ITS zprávy
- Servisní zprávy

Tyto dvě kategorie by měly být na transportní vrstvě odděleny (např. prostřednictvím TCP/UDP portu).

4.5.2.1 C-ITS zprávy

Mezi C-ITS Back Office a C-ITS jednotkami je pro správné fungování systému nutné obousměrně přenášet původní C-ITS zprávy (např. DENM, IVIM). Z důvodu nastavení přísnějších pravidel pro tvorbu C-ITS zpráv z pohledu bezpečnosti je potřeba použít komunikační protokol, ve kterém bude zachována celistvost C-ITS zprávy včetně podpisu zprávy (tzv. securedMessage). Tento požadavek sice stále zanechává jistou volnost, v protokolu však musí být vždy zachovány následující vrstvy:

- Facility vrstva
- Transportní vrstva
- GeoNetworking vrstva



Obrázek 19 Princip hybridního řešení

V rámci této komunikace jsou přenášeny C-ITS zprávy mezi C-ITS Back Office a C-ITS jednotkou / mobilní aplikací prostřednictvím sítí mobilních operátorů nebo pevných datových sítí (v případě komunikace s RSU).

4.5.2.2 Servisní zprávy

Tato kategorie představuje zprávy mezi C-ITS Back Office a C-ITS jednotkou/mobilní aplikací, na které se nevztahuje požadavek na formát C-ITS zpráv dle ETSI standardů. Může se jednat např. o stavové zprávy, systémové nastavení, aj. Pokud mají v dané implementaci servisní zprávy přímý vliv na tvorbu C-ITS zpráv, pak musejí být rovněž podepisovány prostřednictvím rozhraní 4.5.2.1 (obdobně jako C-ITS zprávy).

Předpokládá se, že pro tuto kategorii zpráv bude řešen komunikační protokol proprietárně dle potřeb daného provozovatele či konkrétní implementace.

4.5.3 Rozhraní I3: C-ITS Back Office ↔ Integrovaná platforma

Integrovaná platforma představuje prvek, který zajišťuje propojení C-ITS BO jednotlivých provozovatelů C-ITS a NDIC tak, aby byla zajištěna rychlá a spolehlivá výměna dat mezi jednotlivými prvky.

Provozovatel národní Integrované platformy (ŘSD) definovalo specifikaci komunikačního protokolu mezi C-ITS Back Office a Integrovanou platformou. Detailní specifikace rozhraní je uvedena v dokumentu „IntP – Dokumentace pro připojení subjektů“ [28], který je poskytnut subjektu v rámci procesu registrace k centrálním prvkům.

Jednotlivé subjekty po schválení žádosti o registraci k připojení k centrálním prvkům ze strany provozovatele mohou vysílat a přijímat C-ITS zprávy do/z ostatních C-ITS Back Office. Komunikace mezi C-ITS BO a integrovanou platformou probíhá prostřednictvím protokolu, založeném na technologii HTTP/REST. Zabezpečení komunikace je zajištěno požadavkem na komunikaci s Integrovanou platformou pouze ze schválené veřejné IP adresy, která je uvedena v rámci registrace.

4.5.4 Rozhraní I4: OBU ↔ vozidlové systémy

Toto rozhraní zajišťuje propojení vozidlové C-ITS jednotky systémy vozidla, popř. externí detektory. Systémy, na které se C-ITS jednotka může napojit se liší dle typu vozidla (popř. vozíku), ve kterém je instalována. Tyto systémy představují datové vstupy, které jsou následně použity pro automatické generování specifických C-ITS zpráv, popřípadě jsou tato data přeposílána (viz kap. č.4.5.2) do nadřazených systémů (C-ITS Back Office), kde jsou dále zpracovávána a archivována. U vozidlových jednotek se tak může jednat o následující informační zdroje:

- Palubní LAN síť
- CAN/OBD II sběrnice
- Řídící systémy vozidlových nástaveb
- Odbavovací a informační systémy
- Ovládací systém bezpečnostních vozíků
- Externí detektory
- Manuální vstupy uživatele prostřednictvím HMI



V rámci tohoto rozhraní je řešeno i datové propojení mezi C-ITS jednotkou a HMI zařízením (např. displej, tablet) pro vizualizaci varovných a informačních zpráv pro řidiče.

Toto rozhraní není nutné pro zajištění interoperability C-ITS systému standardizovat a každý subjekt systému si jej vydefiniuje individuálně dle parametrů konkrétní implementace (typ vozidla, potřebný rozsah sledovaných parametrů).

4.5.5 Rozhraní I5: RSU ↔ další zařízení na infrastruktuře

Toto komunikační rozhraní mezi RSU a dalším zařízením (např. řadičem SSZ, ovládací skříň EOV, dopravní detektor) je řešeno proprietárním protokolem výrobce zařízení. Rozsah dat, která jsou přenášena mezi zařízením a RSU jednotkou, je závislý na konkrétní instalaci a rozsahu požadovaných C-ITS služeb.

V textu níže jsou uvedeny ukázky přenášených dat v případě propojení RSU s řadičem SSZ nebo ovládací skříň EOV.

4.5.5.1 Světelné signalizační zařízení

V rámci komunikace RSU → řadič SSZ mohou být přenášeny následující informace:

- Požadavek na prioritní jízdu pro požadovaný směr
- Doplnující informace pro optimalizaci řízení křižovatky (typ vozidla, aktuální poloha, zpoždění oproti JŘ, číslo linky, aj.)

V rámci komunikace řadič SSZ → RSU mohou být přenášeny následující informace:

- Stav žádosti o prioritní jízdu
- Aktuální stav signálů pro jednotlivé směry křižovatky
- Čas do změny fáze
- Obecné stavové informace křižovatky (např. stav řízení křižovatky)

4.5.5.2 Výhybky

V rámci komunikace RSU → ovládací skříň EOV mohou být přenášeny následující informace:

- Požadavek na polohu výhybky z daného směru

V rámci komunikace ovládací skříň EOV → RSU mohou být přenášeny následující informace:

- Aktuální poloha výhybky
- Stav žádosti o přestavení výhybky
- Rychlostní limit pro vjezd do výhybky



- Stavové informace o výhybce (např. funkčnost kolejových obvodů, stav snímačů polohy jazyků výměny, blokování výměny, stav obsazení kapsy, stavy signalizační lampy, havarijní stav – blokování)

4.5.6 Rozhraní I6: C-ITS Back Office ↔ další informační zdroje

Datové rozhraní I6 představuje obecně přímé napojení C-ITS Back Office na množinu systémů, které nejsou přímou součástí C-ITS, ale představují významné datové vstupy pro poskytované služby.

Způsob přenosu ani rozsah přenášených informací není na národní ani mezinárodní úrovni standardizovaný a je na konkrétním zhotoviteli a zadavateli, jak si toto rozhraní definují.

V případě datové komunikace mezi C-ITS Back Office a dopravními řídicími centry, kdy dochází k výměně dopravních informací (data o provozu, mimořádné události, aj.), se doporučuje využít protokol DATEX II, který byl právě pro tyto účely vyvinut a v Evropě je běžně používán. Tento protokol je definován v následujících normativních dokumentech:

- CEN TS 16157-1 Inteligentní dopravní systémy – Specifikace výměnného formátu DATEX II pro řízení dopravy a dopravní informace – Část 1: Obecný rámec a architektura
- CEN TS 16157-2 Inteligentní dopravní systémy – Specifikace výměnného formátu DATEX II pro řízení dopravy a dopravní informace – Část 2: Označování pozice
- CEN TS 16157-3 Inteligentní dopravní systémy – Specifikace výměnného formátu DATEX II pro řízení dopravy a dopravní informace – Část 3: Publikace situace

Překladové tabulky mezi protokoly DATEX II, C-ITS a dalšími (TMC, TPEF2-TEC) jsou zpracovány na evropské úrovni, pod záštitou těchto organizací:

- C2C-CC
- C-Roads
- DATEX II
- TISA
- Data for road safety

4.5.7 Rozhraní I7: C-ITS prvky ↔ PKI CZ

Jedná se o rozhraní mezi security modulem jednotlivých částí C-ITS ekosystému (tj. OBU, RSU, C-ITS Back Office, mobilní aplikace, Integrační platforma) a infrastrukturou bezpečnostní vrstvy. Podoba rozhraní je definována standardy ETSI TS 103 097 a ETSI TS 102 941.

4.5.8 Rozhraní I8: PKI CZ ↔ PKI EU

Rozhraní je definováno provozovatelem evropských centrálních prvků (Společné výzkumné centrum Evropská komise – JRC) do podoby takzvaného CPOC protokolu – C-ITS Point of Contract Protocol. Toto



rozhraní je dostupné na webu JRC (<https://cpoc.jrc.ec.europa.eu/>) a zároveň je využito pro propojení národního PKI (provozovaného ŘSD) s evropskými centrálními prvky.

5 Bezpečnost C-ITS systémů

Bezpečnostní vrstva umožňuje zabezpečenou (důvěryhodnou a spolehlivou) komunikaci v rámci kooperativních inteligentních dopravních systémů. Bezpečnostní vrstva byla provozována během projektu C-Roads Czech Republic, a to formou služby, která byla poskytována pro partnery projektu C-Roads Czech Republic. Během projektu byly stávající C-ITS jednotky (RSU, OBU a RVU) a BO registrovány a autorizovány na serveru PKI. Některé C-ITS jednotky si se serverem PKI vyměňují provozní security metadata a certifikáty napřímo (každá C-ITS jednotka má otevřený přístup z APN na server PKI), jiné prostřednictvím BO (pak je otevřen 1 přístup pro všechny takto připojené jednotky).

Bezpečnost a zejména důvěryhodnost veškerých C-ITS systémů je, s ohledem na jejich heterogenní charakter a distribuovanou architekturu, vystavěna na principech infrastruktury veřejných klíčů (vycházející z angl. ekvivalentu Public Key Infrastructure, dále jen „PKI“), která je technologicky založena na asymetrické kryptografii (často také označované jako kryptografie s veřejným klíčem) a vytváří ekosystém vzájemné důvěry mezi jednotlivými aktéry systému, díky důvěryhodným komponentám a ustanoveným procedurám.

Základ asymetrické kryptografie tvoří dva matematicky vázané kryptografické klíče:

- Soukromý klíč
- Veřejný klíč

Soukromý klíč je důvěrný, slouží pouze jeho vlastníkov, tudíž musí být odpovídajícím způsobem zabezpečen při jeho uchovávání. Druhý z klíčů je veřejný klíč, který mohou používat prakticky všichni, a jeho uchovávání nevyžaduje žádné bezpečnostní prvky. Zásadní vlastností asymetrické kryptografie je nemožnost odvození soukromého klíče pouze ze znalosti veřejného klíče a naopak. Kryptografické operace vždy probíhají s oběma klíči, kdy jedním klíčem je datový obsah šifrován a druhým dešifrován, popřípadě podepisován a ověřován (validován). Pokud se má datový obsah odeslat pouze jedinému příjemci, pak musí být zašifrován veřejným klíčem a k datovému obsahu se pak dostane pouze držitel soukromého klíče, za jehož pomoci lze data dešifrovat.

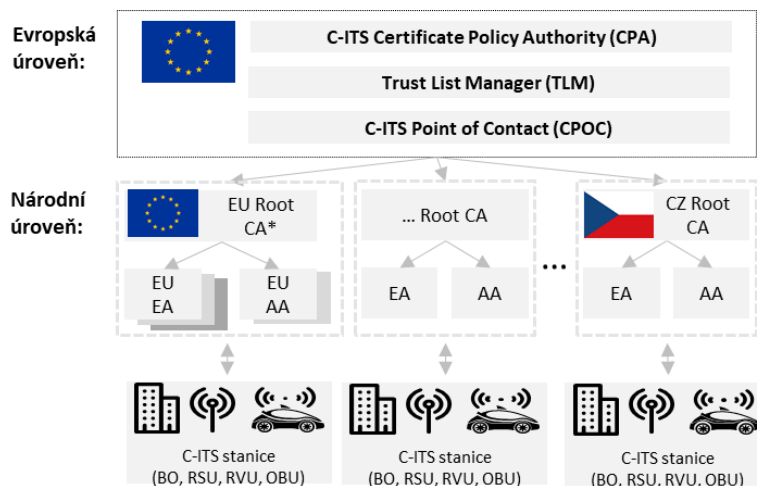
Pro garanci identity odesílatele a zároveň integrity přenášeného datového obsahu je využíván tzv. digitální podpis, kdy se jednocestnou matematickou funkcí z datového obsahu vytvoří její otisk o definované velikosti (častěji v odborné literatuře nazývané jako hash), který je následně zašifrován privátním klíčem odesílatele a připojen k odesílané zprávě.

Příjemce veřejným klíčem odesílající osoby dešifruje digitální podpis, provede rovněž jednocestnou matematickou operaci s přijatým datovým obsahem a vytvoří jeho otisk. Následně oba datové otisky porovná mezi sebou, pokud jsou shodné, pak si může být příjemce jistý, že integrita datové zprávy je zachována (tj. datový obsah nebyl při přenosu upraven) a zároveň je zaručena tzv. nepopíratelnost zprávy, tedy že odesílatelem datového obsahu je držitel privátního klíče.



Distribuovaná architektura C-ITS a zejména jejich mezinárodní interoperabilita dala základ architektuře, která vytváří důvěryhodný ekosystém napříč všemi členskými státy EU, které jsou do C-ITS architektury zapojeny. Architektura systému je rozdělena do dvou základních úrovní:

- Národní úroveň
- Evropská úroveň (evropské centrální komponenty)



Obrázek 20 Základní schéma architektury bezpečnostní vrstvy (zdroj: Koncepce rozvoje C-ITS v ČR)

Celý ekosystém vytváření vzájemné důvěry mezi jednotlivými účastníky C-ITS systémů vychází ze dvou základních evropských dokumentů:

- Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)
- Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

5.1 Národní úroveň

Na národní úrovni fungují jednotlivé PKI systémy, které spravují digitální certifikáty jednotlivých účastníků systému (zajišťují jejich registraci do systému, přidělují odpovídající práva, revokují certifikáty, vydávají CRL), důvěra je zajištěna kořenovou certifikační autoritou, která je nejvyšší důvěryhodná třetí strana v daném systému (který je zpravidla lokální) a dvěma podřízenými certifikačními autoritami, kterým jsou delegovány některé funkcionality (registrační autorita, autorizační autorita). Každé PKI se tak skládá z komponent:

- Kořenová certifikační autorita (dále také „Root CA“ nebo „CA“)
- Registrační autorita (dále také „EA“)
- Autorizační autorita (dále také „AA“)

Základním prvkem architektury PKI zajišťující její důvěryhodnost pro všechny účastníky tzv. certifikační autorita (z angl. ekvivalentu Certification Authority, dále také „CA“). CA je důvěryhodná třetí strana, která garantuje důvěryhodnost celého systému, tj. umožňuje důvěřovat vztahu páru klíčů a jejich držitele (identifikovatelné, resp. identifikované osobě) tím, že veřejně tento vztah deklaruje, ale rovněž je schopna tuto garanci vazby mezi osobou a párem klíčů odvolat. Ačkoliv CA jsou schopny generovat páry klíčů, v mnoha aplikacích tento postup nelze využívat, proto si pár kryptografických klíčů generují účastníci sami a CA pouze generuje elektronické dokumenty (tzv. digitální certifikáty), garantující vztah mezi osobou a veřejným klíčem (tj. jeho držitelem), které jsou elektronicky podepsány certifikační autoritou, resp. jejím privátním klíčem. Certifikát tedy kromě garance vazby příslušného veřejného klíče a jeho vlastníka rovněž umožňuje dovodit vlastnictví odpovídajícího soukromého klíče stejným vlastníkem. Držitelé certifikátu je poskytují jejich uživatelům (nejčastěji příjemcům podepsaných zpráv) prostřednictvím definovaného protokolu, případně jsou tyto certifikáty dostupné v repositáři certifikační autority.

Formát a datová struktura digitálních certifikátů jsou definovány příslušnými normami, kdy jedním ze zásadních parametrů digitálních certifikátů je jejich platnost, která je zpravidla omezena (délka platnosti se stanovuje v závislosti na míře bezpečnostního rizika systému, který PKI využívá). Stejně tak jsou definovány postupy zneplatnění certifikátů, vydávání seznamu zneplatněných certifikátů.

Základními formami vyjádření politiky činnosti CA jsou:

- Certifikační politika (Certificate Policy)
- Certifikační prováděcí směrnice (Certificate Practice Statement).

Tyto dokumenty vytvářejí základ pro zavedení důvěry mezi jednotlivými CA a následné křížové uznávání certifikátů vydaných různými CA.

5.1.1 Kořenová certifikační autorita

Kořenová certifikační autorita (angl. ekvivalent Root CA, dále jen RCA) je základní komponentou bezpečnostní vrstvy, která představuje pro všechny účastníky daného důvěryhodného prostředí (z angl. ekvivalentu trust domain) důvěryhodnou třetí stranu. Jsou jí podřízené registrační a autorizační autority, kterým jsou delegovány specifické služby. Kořenová certifikační autorita je zřízena za účelem:

- Vydávání certifikátů žadatelům o vydání certifikátů
- Zajištění veškerého managementu certifikátů

Vzhledem k tomu, že základem fungování celé bezpečnostní vrstvy je vzájemná důvěra, PKI musí vyhovovat standardním bezpečnostním požadavkům (splňují „Protection Profile“ podle ISO/IEC 15408 Common Criteria for Information Security Evaluation), které jsou ověřovány nezávislým auditorem.



5.1.2 Registrační autorita

Registrační autorita (angl. ekvivalent Enrollment Authority, dále jen EA) představuje podřízenou autoritu kořenové CA, jejíž hlavní funkcí je registrace žadatele o certifikát, resp. ověřování jeho identity, čímž uděluje přístup ke komunikačnímu kanálu. Registrace probíhá mnoha způsoby, zpravidla se však jedná o automatický proces, v některých případech je však nutné realizovat proces registrace manuálně či dávkově.

5.1.3 Autorizační autorita

Autorizační autorita (angl. ekvivalent Authorization Authority, dále jen AA) poskytuje C-ITS stanicím, které jsou registrovány k EA, autorizaci k využívání specifických ITS služeb prostřednictvím autorizačních certifikátů. Autorizace může teoreticky probíhat několika způsoby, v prostředí C-ITS se však zpravidla jedná stejně jako u registrace o automatický proces.

5.2 Evropská úroveň

Evropská úroveň je propojena s národní úrovní a zajišťuje důvěryhodnost mezi jednotlivými lokálními PKI systémy. V C-ITS bezpečnostní architektuře je tak zavedena nadřazená vrstva, zajišťující vzájemnou důvěryhodnost jednotlivých PKI řešení, kterou zajišťují centrální evropské komponenty:

- Trust List Manager (dále také „TLM“)
- C-ITS Point of Contact (dále také „CPOC“).

Jedná se o evropský model důvěryhodnosti C-ITS založený na infrastruktuře veřejných klíčů v rámci celkového systému EU C-ITS Credential Management System (EU CCMS), který definuje právní a technické požadavky na správu certifikátů veřejných klíčů pro aplikace C-ITS vydávajícími subjekty a jejich používání koncovými subjekty v Evropě.

5.2.1 C-ITS Certificate Policy Authority

Nad evropskými komponentami TLM a CPOC leží C-ITS Certificate Policy Authority (dále jen CPA), což je autorita, která je složená ze zástupců veřejných a soukromých subjektů (např. členských států, výrobců vozidel), kteří se podílejí na vytváření a provozu C-ITS důvěryhodného modelu (tzv. Trust Model). CPA odpovídá za dvě dílčí role:

- Správa certifikačních pravidel (z angl. ekvivalentu Certificate Policy Management)
- Správa autorizací PKI

5.2.2 Trust List Manager

Trust list manager (TLM) je centrální komponenta, která je nejvyšším správcem všech kořenových certifikačních autorit, provozovaných v rámci všech zemí EU, kde fungují C-ITS systémy, a to na základě splnění předepsaných pravidel. Tento správce tak vytváří vzájemnou důvěru mezi jednotlivými RCA, a



to prostřednictvím tzv. European Certificate Trust List (ECTL), ve kterém jsou vloženy a zveřejněny certifikáty všech důvěryhodných RCA. Tyto zásady jsou závazné pro všechny subjekty, účastníci se důvěryhodného prostředí C-ITS v Evropě. Důvěryhodnost ECTL závisí jak na nastavených bezpečnostních procedurách, tak do značné míry také na důvěryhodnosti jednotlivých RCA a jejich podřízených CA (EA, AA).

K 5/2021 je v provozu ECTL úrovně L0 (pilotní provoz) a jsou připravovány další prostředí:

- úrovně L1, které bude provozováno s ohledem na požadavky CPA, ale subjekty nebudou muset projít auditem.
- úrovně L2, které bude provozováno s ohledem na požadavky CPA. Subjekty, které se budou chtít připojit budou muset projít auditem.

5.2.3 C-ITS Point of Contact

C-ITS Point of Contact (CPOC) je jedinečná entita jmenovaná CPA. CPOC je centrálním prvkem, který zajišťuje procesy související s distribucí certifikátů mezi TLM a RCA.

6 C-ITS služby

Standardizované C-ITS služby byly rozděleny do několika logických celků na základě jejich funkcí a přínosů, tj.:

- Varování před nebezpečnou lokalitou
 - Varování před stojícím vozidlem
 - Varování před dopravní kongescí
 - Upozornění na dopravní nehodu
 - Varování před počasím boční vítr, srážky, špatná viditelnost
 - Nebezpečí smyku
 - Zvíře/člověk na vozovce
 - Překážka na vozovce
 - špatný technický stav komunikace, nebezpečný směrový oblouk
 - Varování před pomalu jedoucím vozidlem
- Varování před přejezdem a jeho stavem
- Varování před pracemi na silnici
 - Obecné varování před prací na silnici
 - Uzavřený jízdní pruh
 - Uzavřená komunikace
 - Zimní údržba
 - Varování před blížícím se vozidlem údržby
 - Varování před místem zásahu vozidla údržby
- Přenos dopravních symbolů a textových zpráv
- Služby spojené se SSZ
 - Preference vybraných vozidel na SSZ
 - Informace o stavu SSZ
 - Varování před jízdou na červenou
 - Doporučení rychlosti pro plynulý průjezd křižovatkou
- Služby spojené s IZS
 - Varování před blížícím se vozidlem IZS
 - Varování před místem zásahu vozidla IZS
- Bezpečnostní služby MHD
 - Varování před kolizí s vozidlem MHD
 - Varování před vozidlem MHD v zastávce
- Sběr dopravních dat
 - Sběr vozidlových dat
 - Sběr dat z událostí
- Varování před prudkým brzděním



Detailní popis jednotlivých služeb, popis použitých C-ITS zpráv a jejich atributů je uveden v dokumentu „Use Case katalog“, který byl vytvořen v tomto projektu v rámci úkolu 37.1.4. Use Case katalog je průběžně aktualizován tak, aby reflektoval změny v evropských a národních standardech, normách a technických a funkčních specifikacích pan-evropské platformy C-Roads.

Konec dokumentu.