

ISO/TS 16785 - Elektronický výběr poplatků (EFC) - Definice rozhraní mezi DSRC-OBE a vnějšími zařízeními ve vozidle

Aplikační oblast: [Elektronický výběr poplatků \(EFC\)](#)

Rok vydání normy a počet stran: Vydána 2014, 38 stran

Zavedení normy do ČSN: originálem

Rok zpracování extraktu: 2016

Skupina témat: Interoperabilita

Téma normy: Rozhraní komunikační služby

Charakteristika tématu: Definice rozhraní mezi OBU a externími elementy umístěnými ve vozidle

Úvod, vysvětlení východisek
Popis architektury, hierarchie, rolí a vztahů objektů Popis variant modelu mýtného systému za použití různých externích zařízení ve vozidle.
Popis procesu / funkce / způsobu použití Definice základních funkčních celků.
Popis rozhraní / API / struktury systému Definice zpráv a datových elementů.
Definice protokolu / algoritmu / výpočtu
Definice reprezentace dat / fyzikálního významu Reprezentace datových struktur v ASN.1.
Definice konstant / rozsahů / omezení

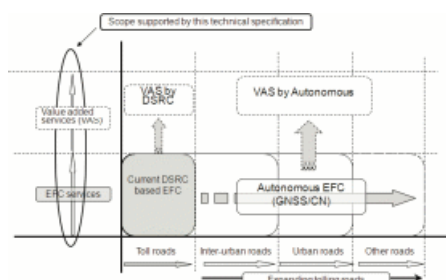
Úvod

Popisovaná technická specifikace se zabývá možným zavedením autonomního [mýtného systému](#) v situaci, kdy určitá část silniční infrastruktury (např. dálnice a rychlostní komunikace) již podléhá [výběru mýtného](#) (založeném na DSRC) a je snaha o rozšíření [výběru](#) na další část silniční infrastruktury. Tato specifikace bere v potaz pouze situaci, kdy je potřeba definovat modelové a komunikační aspekty pro diverzifikované prostředí [EFC systémů](#) – tj. DSRC a autonomní [systémy](#).

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

Užití

Cílem popisovaného dokumentu je nastítnit možné modelové situace, definice datových zpráv a datových elementů pro rozšíření funkcionalit DSRC-OBE v rámci komunikace a kooperace s vnějšími zařízeními ve vozidle. Tato specifikace je tedy vhodná jak pro subjekty pro [výběr mýtného](#), jež plánují rozšíření [mýtné domény](#) pomocí autonomního [EFC systému](#) a poskytují své [OBE](#), tak pro samotné poskytovatele [OBE](#), dodávající [OBE](#) vhodné pro použití v daných [mýtných doménách](#).



Obrázek 1 – Představa rozšíření [služeb](#) a silniční infrastruktury podléhající mýtu (obr. 1 normy)

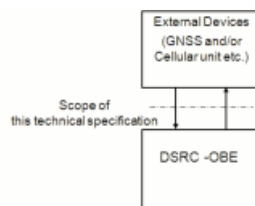
1. Předmět normy

Cílem popisovaného dokumentu je specifikace aplikačního [rozhraní](#) mezi DSRC-OBE a vnějším zařízením ve vozidle, za účelem jejich použitelnosti v diverzifikovaném prostředí [mýtného systému](#) (např. městské či meziměstské komunikace).

Předmět specifikace (obr. 2) zahrnuje zejména následující:

- Definice aplikačního [rozhraní](#) mezi DSRC-OBE a vnějším zařízením ve vozidle (např. GNSS modul, mobilní modul či [rozhraní](#) CAN, atd.)
- Definice datových zpráv a datových elementů pro dané [rozhraní](#)

Z hlediska aplikovatelnosti je obsah této specifikace vhodný jak pro DSRC, tak autonomní [EFC systémy](#), různé prostředí [mýtných systémů](#) a rovněž různé druhy DSRC-OBE založených na různých DSRC normách (CEN, UNİ, ARIB, TTA či GB/T).



Obrázek 2 – Předmět technické specifikace (obr. 2 normy)

2. Související normy

Tato kapitola obsahuje 6 souvisejících norem. Zde jsou uvedeny pouze ty nejdůležitější.

ČSN ISO/IEC 9798-4 (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 4: Mechanismy využívající kryptografickou kontrolní funkci

ČSN EN [ISO 14906](#) (01 8382) Elektronický [výběr mýtného](#) (EFC) – Stanovení aplikačního [rozhraní](#) pro vyhrazené spojení krátkého dosahu

ČSN EN [ISO 17575-1](#) (01 8385) [Elektronický výběr poplatků](#) (EFC) – Definice aplikačního [rozhraní](#) pro autonomní [systémy](#) – Část 1: Zpoplatňování

ČSN EN [ISO 17575-3](#) (01 8385) [Elektronický výběr poplatků](#) (EFC) – Definice aplikačního [rozhraní](#) pro autonomní [systémy](#) – Část 3: [Kontextová data](#)

3. Termíny a definice

Kapitola Termíny a zkratky obsahuje 15 termínů a definic souvisejících s touto normou, z nichž nejdůležitější jsou následující:

[pověření k přístupu](#) (*access credentials*)

data posílaná do [palubního zařízení](#) (OBE), aby byla prokázána deklarovaná identita entity aplikačního procesu zařízení na infrastruktuře (RSE)

[autentikátor, autentizační kód](#) (*authenticator*)

data připojená ke zprávě nebo kryptografická transformace dat, které příjemci dat umožňují ověřit si zdroj a [integritu dat](#), a ochránit tak data proti padělání

[kryptografie](#) (*cryptography*)

vědní obor, který zahrnuje principy, prostředky a metody pro transformaci dat za účelem skrytí jejich informačního obsahu, zabránění jejich neautorizovanému použití, [ověření](#) jejich pravosti, zabránění jejich neodhalenému pozměnění a/nebo zabránění jejich odmítnutí (repudiation)

[vnější zařízení ve vozidle](#) (*external in-vehicle devices*)

zařízení, např. mobilní telefon či dedikovaná jednotka s GNSS a/nebo mobilním modulem, jež jsou připojena k DSRC-OBE za účelem poskytnutí funkcionalit týkajících se aktualizací

Další termíny a zkratky z oboru ITS jsou obsaženy ve [slovníku ITS terminology](#).

4. Symboly a zkratky

Kapitola Zkratky obsahuje 25 zkratk souvisejících s touto normou, z nichž nejdůležitější jsou následující:

ARIB- Asociace telekomunikačního průmyslu a obchodu (*Association of Radio Industries and Business*)

ASN.1- xxxx (*abstract syntax notation one*)

DSRC- vyhrazené spojení krátkého dosahu (*Dedicated Short Range Communication*)

ICC- čipová karta (karta s integrovaným obvodem) (*integrated circuit(s) card*)

PMI- [vydavatel](#) platebních prostředků (*payment means issuer*)

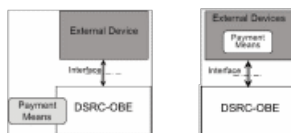
SAM- bezpečnostní aplikační modul (*secure application module*)

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology (www.ITSTERMINOLOGY.org).

5 [Mýtné](#) modely používající vnější zařízení ve vozidle

Tato kapitola prezentuje možné modelové situace použití [mýtných](#) aplikací (t.j. elektronických [mýtných systémů](#)) a vnějších

zařízení ve vozidle. Z hlediska typů platebních účtů se tato kapitola zabývá pouze systémy s uživatelským účtem situovaným přímo ve vozidle (viz obr.3).



Obrázek 3 – Umístění účtu v rámci rozhraní mezi OBE a vnějším zařízením (obr. 5 normy)

Mýtné modely, zmiňované v této kapitole zahrnují následující:

- Mýtné systémy používající DSRC (DSRC-OBE je použita ke všem operacím, např. dobítí kreditu na účtu v mýtném systému)
- Mýtné systémy používající DSRC v kombinaci s mobilním zařízením (např. mobilní telefon za účelem dobítí kreditu účtu v mýtném systému)
- Univerzální mýtný systém, zahrnující jak autonomní systémy, tak systémy používající DSRC v kombinaci vnějším zařízením (např. GPS jednotka, mobilní telefon, pohybové senzory, digitální tachograf).

Tolling services	DSRC-OBE	Components of external in-vehicle devices					
		GNSS	CN device	HEMT	Motion sensors	Digital tachograph	CAN bus unit
1. Basic DSRC tolling	M						
2. Mobile-assisted DSRC tolling	M		M				
3. Universal tolling	M	M	M	M	M	O	O

Tabulka 1 – Přehledová tabulka zařízení a jejich použití v jednotlivých typech modelů (tab. 1 normy)

V rámci popisů jednotlivých modelů je v této kapitole obsažen rovněž stručný popis jednotlivých typů datových zpráv.

6 Datové zprávy

Tato kapitola poskytuje strukturovaný přehled skupin datových zpráv pro komunikaci mezi DSRC-OBE a vnějším zařízením ve vozidle. Jedná se o popis těchto datových skupin:

- Payment means status (datové elementy významné z hlediska platebního módu validace před procesem platby)
- Payment fee (datové elementy spojené s poplatky definované poskytovatelem služeb)
- Account update (datové elementy spojené se způsobem aktualizace kreditu uživatelského účtu v mýtném systému)
- Compliance checking data (datové elementy související s kontrolním procesem fungování jednotky, definované v ISO 12813)
- Location data (datové elementy související s poskytováním lokalizačních dat, definované v ISO 13141).

7 Aspekty týkající se bezpečnosti

Tato kapitola poskytuje hrubý nástin bezpečnostních aspektů týkající se rozhraní mezi DSRC-OBE a vnějším zařízením ve vozidle. Jde zejména o problematiku související s následujícími požadavky uvedenými v normě TS 16439 Elektronický výběr poplatků – Bezpečnostní rámec:

- Přenos dat probíhá pouze mezi autentizovanými entitami
- Přenos dat musí splňovat podmínky integrity a důvěrnosti

Příloha A (normativní) Specifikace datových struktur a typů

Příloha A obsahuje definice datových struktur popsaných v Kapitole 5 a 6 této normy (viz obr. 4).

```

PaymentMeansStatus ::= SEQUENCE{
    paymentMode           Int2,
    accountStatus         AccountStatus,
    paymentMeansBalance   PaymentMeansBalance,
    paymentMeans          PaymentMeans
}

PaymentFee ::= SEQUENCE{
    paymentFeeAmount      Int2,
    paymentFeeUnit        PayUnit
}

```

Obrázek 4 – Příklad definice datových struktur pro status a platbu (text. Přílohy A normy)

Příloha B (normativní) PICS

Příloha B obsahuje PICS šablonu pro front-end za účelem kontroly implementace datových struktur definovaných v Kapitole 5 a 6 této normy.

Příloha C (informativní) Příklad **EFC systému**, využívajícího mobilní platformu

Příloha C obsahuje stručný popis příkladu **EFC systému** (**EFC systém** používající DSRC a implementován v Koreji), jenž používá vnější zařízení (mobilní telefon). Popisuje funkce a procedury pro implementaci **transakce** pro dobítí/odečet kreditu za pomoci technologie Bluetooth.

Příloha D (informativní) Další varianty **EFC systémů**

Příloha D přidává další možné varianty modelů **mýtných systémů** těžících z komunikace mezi DSRC-**OBU** a vnějším zařízením ve vozidle. Jedná se o **systém** umožňující anonymní platbu za pomoci různých platebních mechanismů – např. použití platebních aplikací z tržního prostředí či platba pomocí NFC **rozhraní** mezi RSE a vnějším zařízením.

Příloha D (informativní) Relevantní ITS **služby**

Příloha E prezentuje relevantní ITS **služby**, jež využívají potenciálu kombinace **OBE**-DSRC a vnějšího zařízení ve vozidle. Jedná se zejména o tyto aplikace:

- **Mýtné systémy**
- Dopravní informace (např. dynamická navigace)
- Bezpečnostní asistenční aplikace (např. varování při nebezpečné rychlosti v zatáčce, varování ohledně výskytu překážky na silnici)
- Regulované komerční aplikace (např. monitorování dodržování rychlostních limitů)
- Správa elektrických vozidel (např. monitorování stavu nabíjení baterií).