EXTRAKT z české technické normy

Extrakt nenahrazuje samotnou technickou normu, je pouze informativním materiálem o normě.

35.240.60

Dopravní telematika – Elektronický výběr poplatků – Stanovení aplikačního rozhraní pro vyhrazené spojení krátkého dosahu

ČSN EN ISO 14906

01 8382

Platí od 1.4.2007 120 stran

Úvod

Tato norma specifikuje aplikační rozhraní pro systémy elektronického výběru mýtného (EFC), které využívají vyhrazené spojení krátkého dosahu (DSRC), jak je znázorněno na obrázku 1. Konkrétně stanovuje technické podmínky pro transakční model EFC, datové prvky EFC (zmiňované jako atributy) a funkce, z nichž může být transakce EFC vytvořena v prostředí DSRC.

Tato norma rozlišuje různě vybavená zařízení EFC, OBE či RSE, nepředpokládá se totiž, že každá část zařízení bude obsahovat kompletní sadu funkcí a atributů.

Tato norma je hlavní specifikací v souboru norem pro EFC a má následující strukturu:

V prvních čtyřech kapitolách jsou obsaženy normativní odkazy, definice termínů a zkratky. V kapitole 5 je popsána architektura aplikačního rozhraní EFC, pokud jde o její vztah k architektuře spojení DSRC, včetně adresování atributů dat a složek. Následující kapitola 6 zavádí transakční model EFC, přičemž definuje obecné kroky každé transakce EFC, zvláště ve fázi inicializace. Kapitola 7 a 8 je vyhrazena pro detailní specifikaci aplikačních funkcí EFC a datových atributů EFC. Příloha A (normativní) specifikace použitých datových typů dle ASN.1 (akční parametry a atributy EFC), příloha B (informativní) uvádí příklad transakce založený na specifikace CARDME obsahující specifikaci na bitové úrovni, příloha C (informativní) uvádí příklady transakcí EFC používajících různé funkce a atributy a příloha D (informativní) obsahuje výpis funkčních požadavků, které mohou být zabezpečeny použitím nástrojů poskytnutých v této normě.

Užití

Pro poskytovatele služby tato norma uvádí, jakým způsobem lze dosáhnout vzájemné interoperability mezi dalšími provozovateli a to buď na základě vzájemného uznání proprietárních EFC transakcí obou či více provozovatelů, nebo vytvořením nové společné transakce (funkce). Každý provozovatel musí zvážit, jestli je implementace dodatečných EFC transakcí v možnostech jím provozovaného RSE.

Souvisící normy

Tato norma specifikující rozhraní dodržuje filosofii propojení otevřených systémů (OSI), definovanou v normě ISO/IEC 7498-1, a není závislá na konkrétní implementaci.

1 Předmět normy

Tato norma specifikuje aplikační rozhraní v kontextu systémů elektronického výběru mýtného (EFC), používajících vyhrazené spojení krátkého dosahu (DSRC).

Aplikační rozhraní EFC je rozhraní aplikačního procesu EFC k aplikační vrstvě DSRC, jak je znázorněno na obrázku Obr. 1. Působnost této normy zahrnuje specifikace:

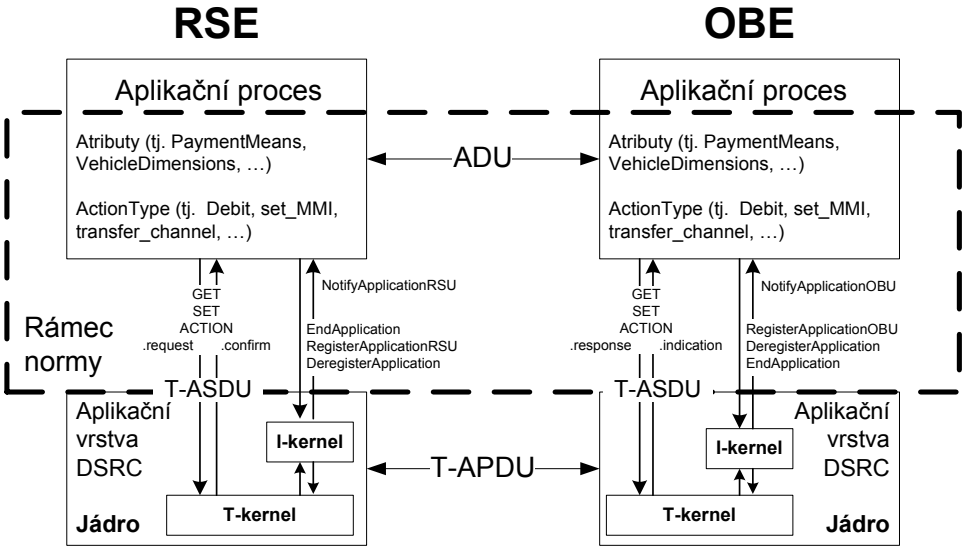
– atributů EFC (tj. informací o aplikaci EFC);

– procedur adresování atributů a (hardwarových) složek EFC (např. ICC a MMI);

– aplikačních funkcí EFC, tj. další kvalifikace akcí pomocí definic příslušných služeb, přidělení přidružených hodnot ActionType a obsahu a významu akčních parametrů;

– transakčního modelu EFC definujícího společné prvky a kroky jakékoliv transakce EFC;

– chování rozhraní tak, aby byla zabezpečena interoperabilita na úrovni aplikačního rozhraní EFC-DSRC.



Obrázek 1 – Aplikační rozhraní EFC

3 Termíny a definice

Norma uvádí 21 termínů a definicí.

3.19 transakce *(transaction)* kompletní výměna informací mezi zařízením na straně infrastruktury (RSE) a palubním zařízením (OBE) nutná pro dokončení EFC operace prostřednictvím DSRC.

4 Zkratky

Kapitola 4 uvádí 31 zkratek. Mezi zásadní patří DSRC (Vyhrazené spojení krátkého dosahu), EFC (elektronické vybírání poplatků), OBE (palubní zařízení), RSE (zařízení na straně infrastruktury) a EID (identifikátor prvku).

5 Architektura

Tato kapitola stanovuje, jaké služby DSRC systém EFC rozeznává, v jakém pořadí je vyvolává a používá k získání či změně atributů uložených v OBE. Vše se děje za účelem správného a účelného zpoplatnění cesty. Mezi základní používané služby patří funkce GET, SET, ACTION, EVENT-REPORT a INITIALISATION, k těmto službám jsou uvedené konkrétní příklady využití. Dále tato kapitola stanovuje způsob jakým RSE přistupuje k datům (atributům) uloženým v OBE a zavádí koncept jmenných prostorů tak, aby bylo možné v jednom OBE mít více stejných atributů oddělených od sebe právě zařazením do jiných jmenných prostorů prostřednictvím parametru ContextMark nesoucího identifikátor EID. Pro adresování jednotlivých komponent OBE (čipové karty, GPS jednotky, displeje, atd.) jsou zde stanoveny funkce SET_MMI a TRANSFER_CHANNEL.

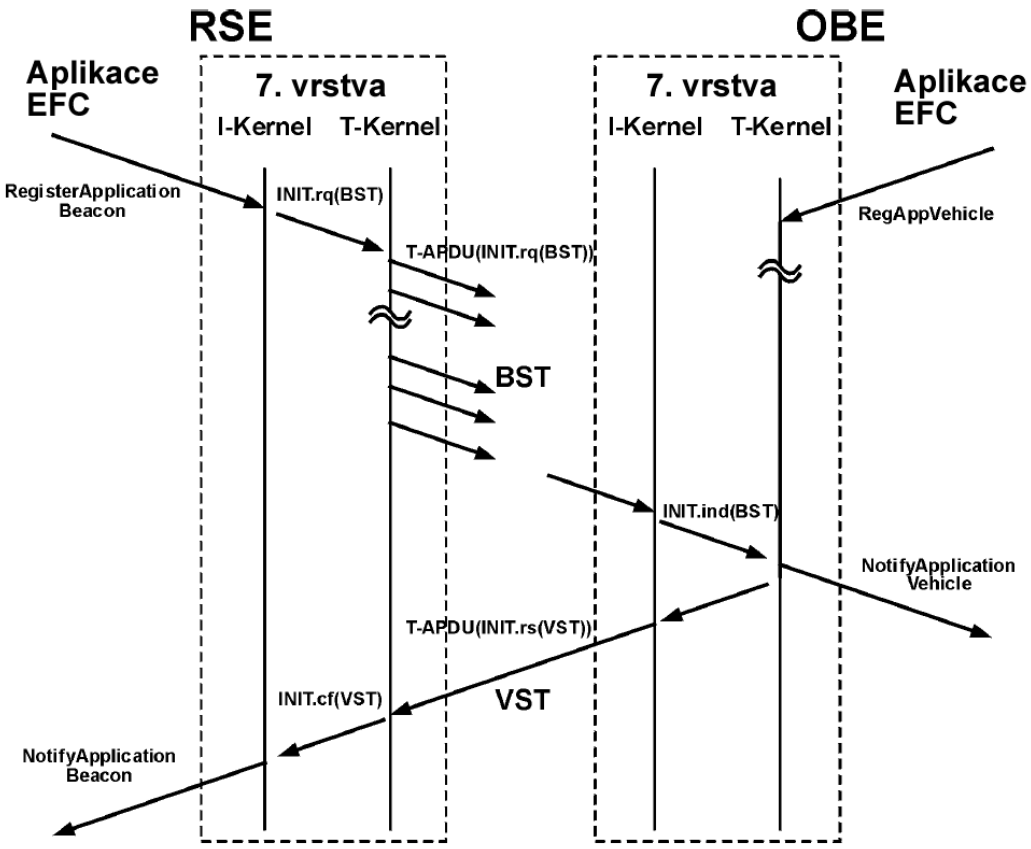
6 Transakční model

Tato kapitola podrobně rozebírá tzv. transakční model, který se skládá ze dvou fází: inicializační a vlastní transakční fáze. Inicializační fáze je založena na výměně informačních tabulek o tom, jaké služby, funkce a atributy jsou podporovány v zařízení ve vozidle (OBE) a zařízení na infrastruktuře (RSE). Informační tabulky jsou nazývány BST resp. VST a v této kapitole je stanoven specifický obsah těchto tabulek pro aplikaci EFC. V transakční fázi dochází k využití společných služeb (identifikovaných v rámci inicializační fáze) za účelem započtení průjezdu placenou zónou a výměně nejen platebních instrukcí, ale i bezpečnostních prvků tak, aby byla znemožněna následná manipulace se záznamem. Tato kapitola nestanovuje explicitně konkrétní postupy a použité funkce, to závisí na implementaci a měl by to provést provozovatel služby.

Transakce se může skládat z těchto kroků:

– GET(EID, ContractValidity, ContractVehicle, ReceiptServicePart, PaymentMeansBalance)

– DEBIT(EID, DebitPaymentFee)
– SET(EID, ReceiptServicePart)



Obrázek 2 – Inicializační fáze: výměna tabulek BST a VST

7 Funkce EFC

Tato kapitola popisuje funkce EFC vyvolané přes DSRC spojení, mezi komunikujícími aplikacemi. Každá funkce EFC se skládá z páru základů služby; požadavku a jemu odpovídající odezvě. V následující tabulce je uveden jejich výčet, každá funkce je v normě podrobně popsána (jaké jsou její proměnné, kdy je používána, atd.)

Tabulka 1 – Přehled funkcí EFC

jméno funkce	**popis**
GET_STAMPED	získá data s autentikátorem z OBE
SET_STAMPED	nastaví v OBE data, generující autentikátor
GET_SECURE	bezpečně přenese data z OBE
SET_SECURE	bezpečně nastaví data v OBE
GET_INSTANCE	získá řadu položek z více instancí atributu
SET_INSTANCE	nastaví jeden záznam na konkrétní pozici ve více instancích atributu
GET_NONCE	získá hodnotu „nonce“, obvykle se používá proti útokům v odpovědi
SET_NONCE	nastaví hodnotu „nonce“, obvykle se používá proti útokům v odpovědi
TRANSFER_CHANNEL	nastaví či (a) získá data z adresované součásti OBE (např. ICC)
COPY	zkopíruje data ze zdrojového EID do cílového EID
SET_MMI	vyvolá funkci MMI (např. signál OK prostřednictvím bzučáku)

jméno funkce	popis
SUBSTRACT	odečte danou hodnotu od adresované hodnoty
ADD	přidá danou hodnotu k adresované hodnotě
DEBIT	debetní peněženka
CREDIT	kreditní peněženka
ECHO	OBE vrací nazpět přijatá data (echo)

8 Atributy EFC

Tato kapitola popisuje veškeré možné atributy EFC, jejich název, účel, datový obsah, povolenou délku v bytech a skupinu, do které atributy patří. V normě je takto stanoveno 36 atributů, mezi které patří například „platnost kontraktu“, „stav vybavení“ či „počet náprav vozidla“, tyto atributy spadají do následujících kategorií: Kontrakt (Contract), Stvrzenka (Receipt), Vozidlo (Vehicle), Vybavení (Equipment), Řidič (Driver) a Platba (Payment).

Tabulka 36 – Atributy EFC (část tabulky)

AttributeID	atribut	délka v slovech	skupina dat
0	EFC-ContextMark	6	Contract
1	ContractSerialNumber	4	
2	ContractValidity	6	
3	ContractVehicle	Proměnná	
4	ContractAuthenticator	Proměnná	
5	ReceiptServicePart	13	Receipt
6	SessionClass	2	
7	ReceiptServiceSerialNumber	3	
9	ReceiptContract	9	
10	ReceiptOBUId	Proměnná	
11	ReceiptICC-Id	Proměnná	
12	ReceiptText	Proměnná	
13	ReceiptAuthenticator	Proměnná	
14	ReceiptDistance	3	
15	VehicleIdentificationNumber	Proměnná	Vehicle

Tabulka 38 – Datová skupina RECEIPT (stvrzenka) – (ukázka atributu receipt distance)

atribut EFC	Stanovení	typ	bytů	rozsah	poznámka
ReceiptDistance	Celková vzdálenost ujetá vozidlem od počátku jeho existence. Jednotky vzdálenosti jsou 100 metrů.	INT3	3	0.. 16777215	Záznamy o ujeté vzdálenosti (například z tachografu) mohou být použity pro výpočet poplatku PaymentFee založeném na ujeté vzdálenosti.

Příloha A (normativní) Specifikace datových typů EFC

Tato příloha uvádí specifikaci použitých datových typů podle ASN.1 (akční parametry a atributy EFC) tak, aby je bylo možné importovat do dalších aplikačních modulů a norem dopravní telematiky.

Příloha B (informativní) Transakce CARDME

Tato příloha poskytuje příklad transakce prostřednictvím specifikace transakce CARDME. V části B.2 je nejprve uveden přehled průběhu transakce. Její fáze a výměny dat jsou následně stanoveny v části B.3. Nakonec, v části B.4, je vysvětleno přesné stanovení na úrovni bitů. Jedná se o konkrétní příklad určený pro lepší pochopení normy.

Tabulka B.1 – 4 fáze transakce CARDME

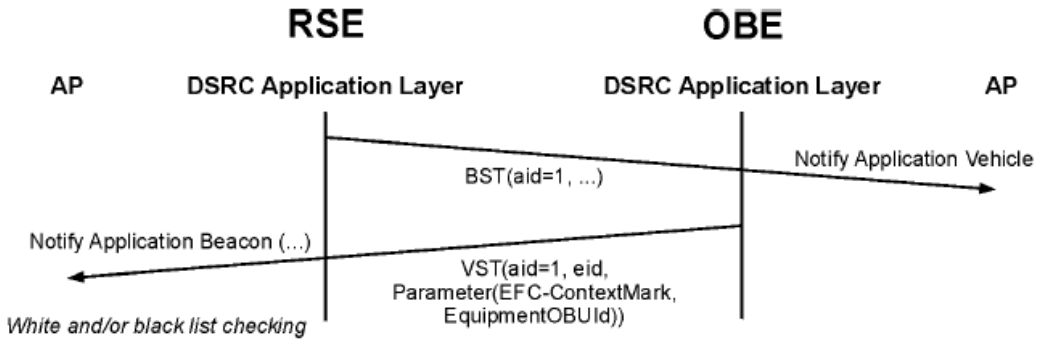
Fáze	Ikona	Stručný popis
Inicializace		**„Dobrý den, vítejte, odkud jedete, jakým způsobem chcete provést platbu“** Jednání o užití určitého EFC kontraktu
Představení		**„Prosím předložte informace potřebné k platbě a vstupní lístek“** RSE načte data o OBE (detaily o smlouvě, účtu, klasifikaci vozidla, poslední transakci, apod.)
Stvrzenka		**„Zde je vaše stvrzenka“** RSE vypíše elektronickou stvrzenku, která může sloužit i jako vstupní karta
Sledování, uzavření		**„Děkujeme, nashledanou“** RSE sleduje vozidlo komunikační zónou a nakonec uzavře transakci

Příloha C (informativní) Příklady typů transakcí EFC

V příloze C jsou obsaženy informativní příklady různých typů transakcí EFC za použití specifických EFC funkcí a atributů ustanovených v této normě. Příklady jsou pro tyto typy transakcí: EFC transakce pouze pro čtení; EFC transakce pro čtení i zápis; transakce elektronické peněženky EFC používající funkci DEBIT; transakce elektronické peněženky EFC používající funkci TRANSFER_CHANNEL a EFC transakce používající více kontraktů. Důvod těchto příkladů je demonstrovat koncept různých transakcí a ukázat, jak jsou zavedeny v této normě.

Pro ilustraci je uveden jednoduchý příklad EFC transakce pouze pro čtení.

Příklad popsaný na obrázku C.1 je založen na centrálním záznamu transakce pouze pro čtení bez jakýchkoliv bezpečnostních opatření.



Obrázek C.1 – EFC transakce pouze pro čtení

Příloha C uvádí příklady různých transakcí na celkem 17 obrázcích.

Příloha D (informativní) Funkční požadavky

Příloha D obsahuje funkční požadavky použité pro validaci první verze této normy. Požadavky byly identifikovány vyhodnocením řady připomínek a poznámek, od různých evropských či mimo-evropských operátorů, popisujících různé transakční profily a modely.

Základní požadavky jsou seskupeny do těchto 7 rozdílných funkčních oblastí.

– Typy transakcí,

– Typy plateb,

– Typy kontraktů,

– Nakládání s kontraktem,

– Bezpečnostní pravidla,

– Provozní záležitosti a

– Tarifní schémata.

Každá funkční oblast obsahuje řadu základních funkčních požadavků. Detaily těchto požadavků jsou uvedeny v následujících tabulkách, které obsahují stručný popis požadavku a případně i příklad použití.

Pro ilustraci je uvedena část tabulky D.1

Tabulka D.1 – Typy transakcí

položka	popis	příklad
vstupní transakce uzavřeného mýtného systému	transakce nastávající při vstupu do uzavřeného mýtného systému	
výstupní transakce uzavřeného mýtného systému	transakce nastávající při výstupu z uzavřeného mýtného systému	
transakce otevřeného mýtného systému	transakce nastávající na stanici otevřeného mýtného systému	
průjezdní transakce	transakce čtení a zápisu nastávající při průjezdu OBE určitou částí silniční sítě	používá se pro identifikaci průjezdu specifické OBE skrz daný výsek komunikace a v důsledku k identifikaci použité silnice mezi dvěma různými body.
kontrolní transakce	transakce sloužící ke kontrole správného provedení transakce; je založena na zabezpečeném čtení.	používá se ke kontrole správnosti provedení poslední zaznamenané transakce za účelem prosazování zákona (enforcement).