EN ISO 14906 - **Elektronický výběr poplatků (EFC) – Stanovení aplikačního rozhraní pro vyhrazené spojení krátkého dosahu (DSRC)**

Aplikační oblast: Elektronický výběr poplatků (EFC)

Rok vydání normy a počet stran: Vydána 2018, 123 stran

Rok zpracování extraktu: 2021

Skupina témat: Mýtné používající DSRC

Téma normy: Rozhraní komunikační služby

Charakteristika tématu: Definice komunikačního rozhraní mezi OBU a RSE v rámci mýtného systému.

Úvod, vysvětlení východisek

Popis významu normy ve vztahu k interoperabilitě mýtných systémů.

Popis architektury, hierarchie, rolí a vztahů objektů

Identifikace a popis aplikačního rozhraní mezi OBE a RSE v rámci architektury EFC systémů. Informativní popis transakcí za použití různých funkčních primitiv.

Popis procesu / funkce / způsobu použití

Definice obecného transakčního modelu pro EFC službu včetně jednotlivých fází - inicializační a transakční.

Popis rozhraní / API / struktury systému

Jména a popis API funkcí společně s jejich parametry. Definice zpráv a datových elementů a způsobu jejich adresování.Požadavky na služby nižších vrstev. Definice bezpečnostních mechanismů použitých v rámci transakcí.

Definice protokolu / algoritmu / výpočtu

Definice reprezentace dat / fyzikálního významu

Reprezentace datových struktur v ASN.1.

Definice konstant / rozsahů / omezení

Úvod

Tato technická norma (dále rovněž “popisovaný dokument”) specifikuje aplikační rozhraní pro systémy elektronického výběru mýtného (EFC), které využívají vyhrazené spojení krátkého dosahu (DSRC). Konkrétně stanovuje technické podmínky pro transakční model EFC, funkce EFC a datové atributy EFC, ze kterých může být transakce EFC vytvořena v prostředí DSRC.

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

Užití

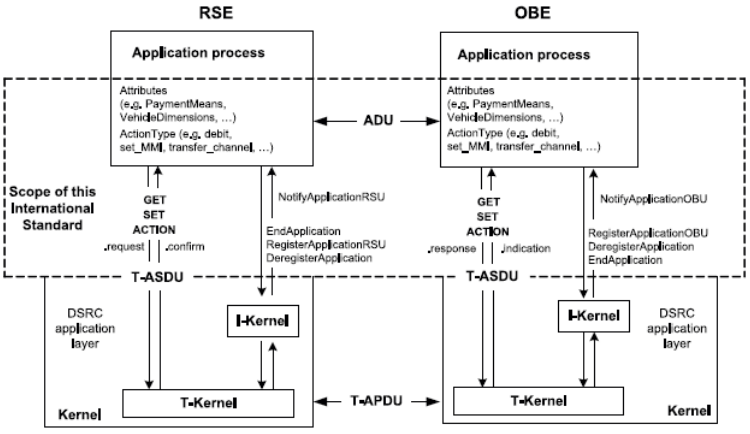
Popisovaný dokument je určený pro provozovatele mýtných systémů postavených na technologii DSRC a rovněž pro poskytovatele mýtných služeb. Popisovaný dokument stanovuje základní prvky vzájemné interoperability komponent systémů elektronického výběru mýtného, konkrétně palubního zařízení (OBE) a zařízení na infrastruktuře (RSE).

1. Předmět normy

Popisovaný dokument specifikuje aplikační rozhraní pro systémy elektronického výběru mýtného, které využívají technologie DSRC. Aplikační rozhraní představuje rozhraní aplikačního procesu EFC k aplikační vrstvě DSRC, jak je

znázorněno na Obrázku 1. Dokument předkládá specifikaci:

- datových atributů EFC, tj. informací o aplikaci EFC;
- procedur adresování atributů a (hardwarových) komponent EFC (např. ICC a MMI);
- aplikačních funkcí EFC, tj. další kvalifikaci akcí pomocí definic příslušných služeb;
- transakčního modelu EFC definujícího společné prvky a kroky jakékoliv transakce EFC;
- chování rozhraní tak, aby byla zabezpečena interoperabilita na úrovni aplikace EFC a aplikačního rozhraní DSRC;



Obrázek 1 – Rozsah popisovaného dokumentu (obr. 1 normy)

2. Souvisící normy

Popisovaný dokument se odkazuje na 12 technických norem, z nichž nejdůležitější jsou:

ISO/IEC 9797-1, Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MAC) — Část 1: Mechanismy používající blokovou šifru

ISO 15628, Inteligentní dopravní systémy — Vyhrazené spojení krátkého dosahu (DSRC) – Aplikační vrstva

3. Termíny a definice

Tato kapitola obsahuje 17 termínů a definic souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou:

atribut (attribute) – adresovaný balíček dat tvořený jedním nebo posloupností více datových prvků

palubní zařízení (on-board equipment) – zařízení instalované ve vozidle vykonávající požadované funkce EFC

zařízení na infrastruktuře (roadside equipment) – zařízení umístěné podél infrastruktury vykonávající požadované funkce EFC

transakce (transaction) – kompletní výměna informací mezi zařízením na infrastruktuře (RSE) a palubním zařízením (OBE)

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology.

4. Symboly a zkratky

Tato kapitola obsahuje 35 zkratek souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou následující:

DSRC vyhrazená komunikace krátkého dosahu (dedicated short-range communications)

EFC elektronický mýtný systém; elektronický výběr mýtného (electronic fee collection)

OBE palubní zařízení (on-board equipment)

RSE zařízení na infrastruktuře (roadside equipment)

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

5 Architektura aplikačního rozhraní DSRC

Tato kapitola v rozsahu 5 stránek stanovuje, jaké služby aplikačního rozhraní DSRC systém elektronického výběru mýtného rozeznává, v jakém pořadí je vyvolává a jak je používá k získání či změně atributů uložených v palubním zařízení. Mezi základní používané služby patří funkce GET, SET, ACTION, EVENT-REPORT a INITIALISATION.

Dále tato kapitola stanovuje způsob, jakým zařízení na infrastruktuře (RSE) přistupuje k datovým atributům uloženým v palubním zařízení (OBE). Je zde zaveden koncept jmenných prostorů, aby bylo možné v jednom palubním zařízení odděleně uchovávat více sad atributů, každou pro použití v jiné mýtné doméně. Identifikace každého jmenného prostoru je uskutečňována prostřednictvím atributu EFC-ContextMark.

6 Transakční model EFC

Tato kapitola v rozsahu 5 stránek stanovuje transakční model EFC skládající se ze dvou fází – inicializační a transakční.

Inicializační fáze je založena na výměně zpráv s parametry vysílače a vozidla (tzv. BST a VST), v rámci kterých jsou předávány informace o službách, funkcích a atributech, které jsou podporovány palubním zařízení (OBE) a zařízením na infrastruktuře (RSE). V této kapitole je stanoven specifický obsah těchto tabulek pro aplikaci EFC.

Během transakční fáze dochází k využití služeb identifikovaných v rámci inicializační fáze za účelem registrace průjezdu zpoplatněným úsekem a výměně informací pro stanovení mýtného, ale i bezpečnostních prvků tak, aby byla znemožněna následná manipulace se záznamem.

7 Funkce EFC

Tato kapitola v rozsahu 2 stránek popisuje funkce aplikačního rozhraní DSRC definovaných pro aplikaci EFC. Celkem je zde popsáno 16 funkcí, které jsou vyjmenovány v následující tabulce. Každá funkce se skládá z páru základů služby, tj. požadavku a odpovědi, jejichž parametry jsou v této kapitole podrobně popsány.

Function name	Action type	Action parameter	Response parameter	Remarks
GET_STAMPED	0	GetStampedRq	GetStampedRs	retrieves data with an authenticator from the OBE
SET_STAMPED	1	SetStampedRq	OCTET STRING	sets data in the OBE, which generates an authenticator
GET_SECURE	2	OCTET STRING	OCTET STRING	gets data securely from the OBE
SET_SECURE	3	OCTET STRING	OCTET STRING	sets data securely in the OBE
GET_INSTANCE	4	GetInstanceRq	GetInstanceRs	retrieves a number of entries out of an attribute's multiple instances
SET_INSTANCE	5	SetInstanceRq	n.a.	sets one entry at a specified position in an attribute's multiple instances
GET_NONCE	6	n.a.	OCTET STRING	retrieves a nonce - typically used against replay attacks
SET_NONCE	7	OCTET STRING	n.a.	sets a nonce - typically used against replay attacks
TRANSFER_CHANNEL	8	ChannelRq	ChannelRs	sets and/or retrieves data from the addressed OBE component (e.g. an ICC)
COPY	9	CopyRq	n.a.	copies data from a source EID to a destination EID
SET_MMI	10	SetMMIRq	n.a.	invokes an MMI function (e.g. signal Ok via buzzer)
SUBTRACT	11	SubRq	n.a.	subtracts the given value to the addressed value
ADD	12	AddRq	n.a	adds the given value to the addressed value
DEBIT	13	DebitRq	DebitRs	debits purse
CREDIT	14	CreditRq	CreditRs	credits purse
ECHO	15	OCTET STRING	OCTET STRING	OBE echoes received data

Tabulka 1 – Přehled funkcí aplikačního rozhraní DSRC (tab. 1 normy)

8 Atributy EFC

Tato kapitola v rozsahu 24 stránek popisuje všechny datové atributy EFC, jejich název, účel a datový obsah, tj. soupis datových prvků tvořící daný atribut. Pro jednotlivé prvky je zde uvedena jejich definice, datový typ dle ASN.1, povolená délka v bytech a povolený rozsah hodnot. V popisovaném dokumentu je specifikováno celkem 47 atributů, které jsou rozřazeny do následujících datových skupin – smlouva, stvrzenka, vozidlo, vybavení, řidič a platba. Jedná se o stěžejní kapitolu popisovaného dokumentu.

Příloha A (normativní) – Specifikace datových typů EFC

Příloha A v rozsahu 1 stránky uvádí specifikaci použitých datových typů podle ASN.1. Je zde uveden odkaz na příslušné ASN soubory, které je možné importovat do dalších aplikačních modulů.

Příloha B (informativní) – Transakce CARDME

Příloha B v rozsahu 34 stránek poskytuje informativní příklad transakce prostřednictvím specifikace transakce CARDME. V první části je představen průběh transakce rozdělený do těchto fází:

- inicializace (inicialization), kdy OBE předá RSE informaci o smlouvě;
- provedení (presentation), kdy RSE načte informace o OBE (detaily o smlouvě, účtu, klasifikaci vozidla, poslední transakci apod.);
- potvrzení (receipt), kdy RSE předá OBE elektronickou stvrzenku;
- sledování a uzavření (tracking and closing), kdy RSE sleduje vozidlo v komunikační zóně a následně transakci uzavře;

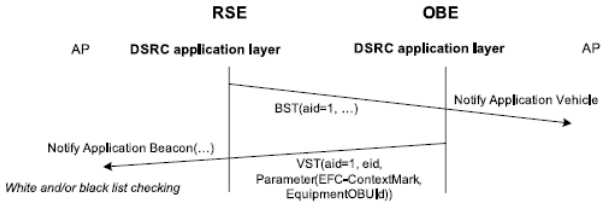
V další části této přílohy jsou jednotlivé fáze popsány z pohledu výměny dat a závěrem je zde pro jednotlivé fáze uvedena specifikace na úrovni bitů.

Příloha C (informativní) – Příklady typů transakcí EFC

Příloha C v rozsahu 12 stránek poskytuje informativní příklad různých typů transakcí EFC za použití specifických EFC funkcí a atributů ustanovených v tomto popisovaném dokumentu. Příklady jsou uvedeny pro následující typy transakcí:

- transakce EFC pouze pro čtení;
- transakce EFC pro čtení a zápis;
- transakce elektronické peněženky EFC používající funkci DEBIT;
- transakce elektronické peněženky EFC používající funkci TRANSFER_CHANNEL;
- transakce EFC používající více kontraktů;

Tato příloha má za cíl demonstrovat koncept různých transakcí a ukázat, jak jsou v popisovaném dokumentu zavedeny. Pro ilustraci je níže uveden příklad transakce EFC pouze pro čtení.



Obrázek 2 – Transakce EFC pouze pro čtení (obr. C.1 normy)

Příloha D (normativní) – Mapovací tabulka mezi znakovými sadami

Příloha D v rozsahu 1 stránky stanovuje mapovací pravidla pro převod znaků ISO 8859-2 (Latin2, Východoevropská) znakové sady a ISO 8859-5 (Cyrilice) znakové sady do ISO 8859-1 (Latin1, Západoevropská) znakové sady.

Příloha E (informativní) – Mapovací tabulka pro atributy vozidla

Příloha E v rozsahu 3 stránek stanovuje mapovací pravidla mezi atributy zaznamenanými v osvědčení o registraci vozidla a atributy EFC definovanými tímto popisovaným dokumentem. Cílem této přílohy je usnadnit personalizaci OBE údaji o vozidle. Pro ilustraci je níže uvedeno mapování pro několik těchto atributů.

AttributeId	EFC Attribute	Data Element	Registration certificate element	
15	VehicleIdentificationNumber	VehicleIdentificationNumber	(E)	vehicle identification number;
16	VehicleLicensePlateNumber	VehicleLicencePlateNumber	(A)	registration number;
17	VehicleClass	VehicleClass	(J)	vehicle category;
19	VehicleAxles	VehicleAxlesNumber	(L)	number of axles;
20	VehicleWeightLimits	VehicleMaxladenWeight	(F.2)	maximum permissible laden mass of the vehicle in service in the Member State of registration;

Tabulka 2 – Mapovací tabulka pro atributy vozidla (ukázka tab. E.1 normy)

Příloha F (normativní) – Bezpečnostní výpočty podle DES

Příloha F v rozsahu 5 stránek obsahuje detailní definici bezpečnostních výpočtů podle standardu pro šifrování dat (DES).

Příloha G (informativní) – Příklad bezpečnostních výpočtů podle DES

Příloha G v rozsahu 3 stránek uvádí celkem 4 numerické příklady bezpečnostních výpočtů podle standardu pro šifrování dat (DES).

Příloha H (normativní) – Bezpečnostní výpočty podle AES

Příloha H v rozsahu 5 stránek obsahuje detailní definici bezpečnostních výpočtů podle pokročilého standardu pro šifrování dat (AES).

Příloha I (informativní) – Příklad bezpečnostních výpočtů podle AES

Příloha I v rozsahu 2 stránek uvádí celkem 4 numerické příklady bezpečnostních výpočtů podle pokročilého standardu pro šifrování dat (AES).