EXTRAKT z české technické normy

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

35.240.60

Dopravní telematika – Elektronický výběr poplatků – Interoperabilita DSRC: Aplikační profil

ČSN EN 15509

01 8386

Platí od 1.11.2007

59 stran

Úvod

Tato norma definuje interoperabilní aplikační profil pro transakce v rámci DSRC–EFC. Jejím hlavním cílem je podporovat technickou interoperabilitu mezi EFC systémy. Aplikační profil je referenční implementací systému výběru poplatků.

Tato norma definuje pouze základní úroveň technické interoperability pro zařízení EFC (palubní jednotku OBU a zařízení na pozemní komunikaci RSE, které spolu komunikují prostřednictvím DSRC). Neposkytuje úplné řešení pro interoperabilitu a ani nedefinuje aspekty týkající se např. ostatních částí EFC systému, jiných služeb, jiných technologií a netechnických prvků interoperability.

Norma vychází z výsledků evropských projektů jako jsou CARDME, PISTA a CESARE, neboť tyto představují plody evropské harmonizace EFC a byly použity jako základ v několika národních implementacích.

Interoperabilní aplikační profil je definován pomocí požadavků na shodu zařízení, které jsou uvedeny v kapitole 5. Pro usnadnění odkazování, zkoušení a vyhledávání jsou tyto požadavky rozděleny do dvou částí; požadavky na palubní jednotku (OBU) (článek 5.1) a požadavky na zařízení na pozemní komunikaci (RSE) (článek 5.2).

Dále norma také zahrnuje různé přílohy udávající podrobné specifikace i pozadí, motivaci a příklady požadavků na shodu. Záměrem je, aby tyto přílohy podpořily čitelnost a srozumitelnost této normy.

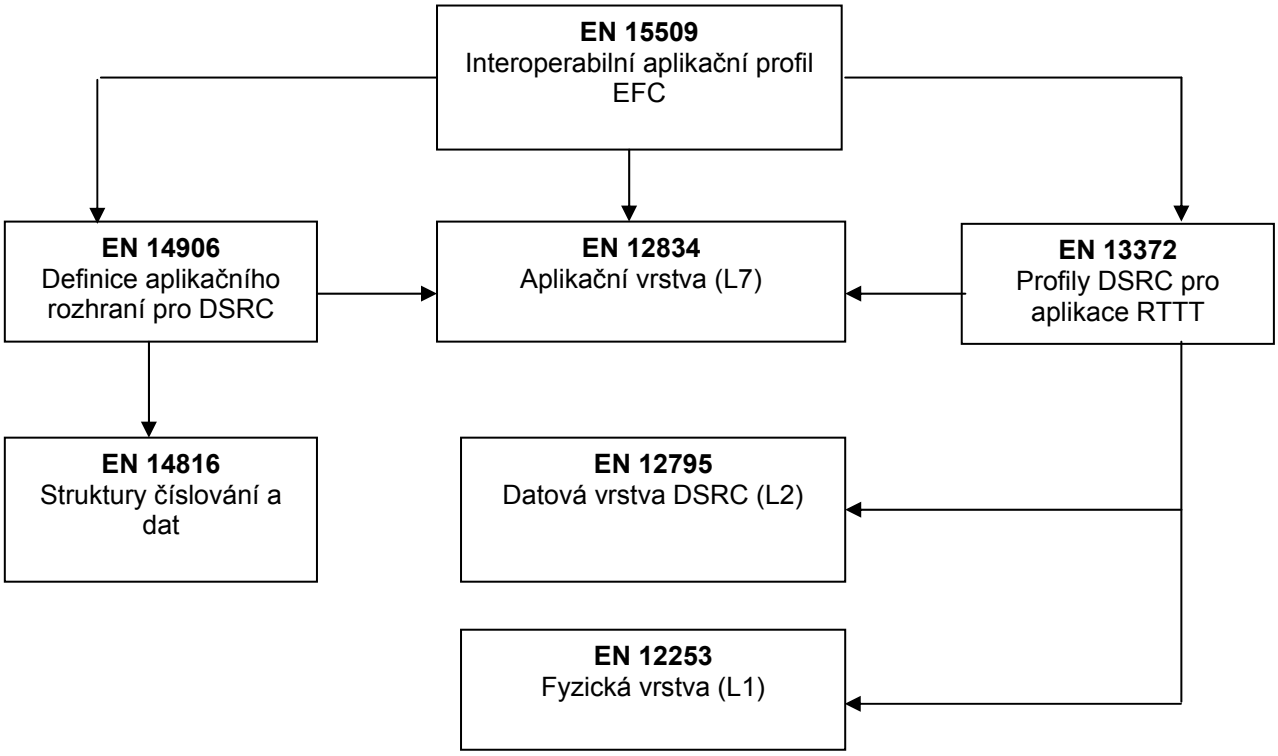
Užití

Operátoři, vydavatelé a výrobci mohou používat aplikační profil jako základ pro interoperabilní využití svých zařízení bez nutnosti zásahů do lokálně využívaného systému EFC. Tato norma se používá pouze na zařízení EFC pro interoperabilní transakce. Tato norma ponechává plnou flexibilitu pro navrhování a implementaci lokálních systémů přímo podle základních norem.

Souvisící normy

Aplikační profil je popsán pomocí konceptu „Mezinárodní normalizované profily (ISP)“, jak jsou definované v ISO/IEC TR 10000-1. Koncept ISP je speciálně navržen pro definování interoperabilních specifikací, kde sadu základních norem lze použít různými způsoby. To je přesně případ EFC, kde sada základních norem uvádí několik různých výběrů parametrů.

Normu lze používat pouze v kontextu jiných norem, jak uvádí obrázek 3.



Obrázek 3 – Odkazy mezi základními normami a normou aplikačního profilu (touto normou)

1 Předmět normy

Předmět této normy se omezuje na:

– Platební metodu: Centrální účet zakládající se na EFC–DSRC.

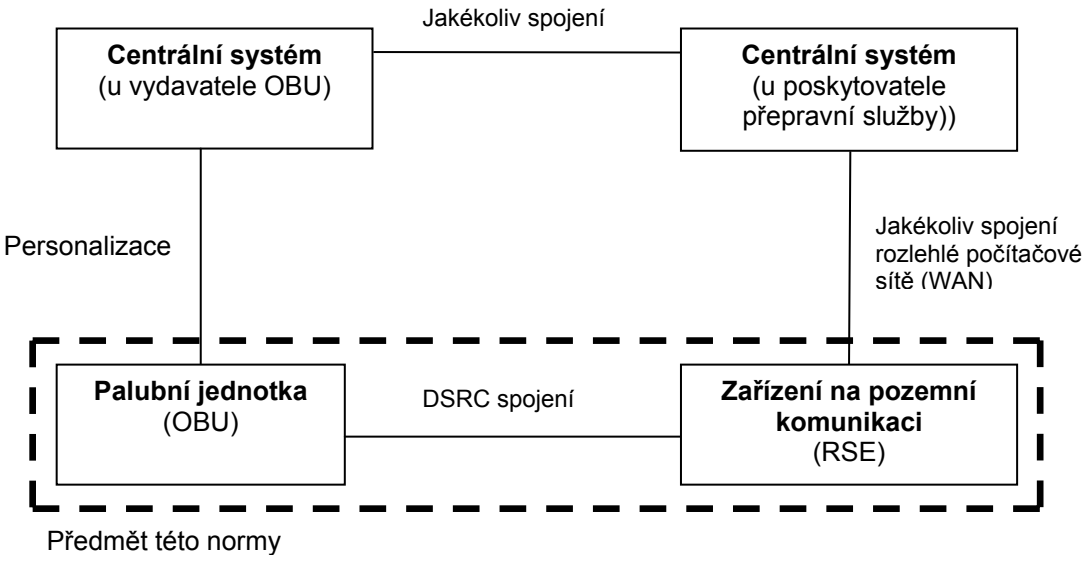
– Fyzické systémy: Palubní jednotka OBU, zařízení na pozemní komunikaci RSE a jejich rozhraní (všechny funkce a informační toky související s těmito částmi systému).

– Požadavky na DSRC spojení.

– EFC transakce (pro rozhraní OBU a RSE).

– Datové prvky využívané OBU a RSE.

– Bezpečnostní mechanismy pro OBU a RSE.



Obrázek 1 – Předmět této normy (a fyzická architektura)

3 Termíny a definice

Norma uvádí 28 termínů a definicí většinou identických s terminologií specifikace EN 14906.

3.1 pověření k přístupu *(access credentials)* data posílaná do palubního zařízení (OBE) tak, aby byla zajištěna identita aplikačního procesu pro zařízení na pozemní komunikaci (RSE)

POZNÁMKA Pověření k přístupu obnáší údaje potřebné pro splnění podmínek vstupu, aby mohlo dojít k procesu na požadovaném prvku v OBE. Pověření k přístupu může obsahovat heslo nebo zašifrovaný údaj jako např. ověřovatele.

3.4 ověřovatel *(authenticator)* data přidaná ke zprávě nebo kryptografická transformace dat, která umožňuje příjemci dat si ověřit zdroj a integritu dat a ochránit tak data proti padělání

3.13 mezinárodní normalizovaný profil *(International Standardised Profile)* mezinárodně odsouhlasený a harmonizovaný dokument, který popisuje jeden nebo více profilů [ISO/IEC TR 10000]

3.15 vydavatel *(issuer)* subjekt zodpovědný za platební systém a za vydávání platebních prostředků uživatelům

3.16 palubní zařízení *(on–board equipment)* zařízení spojené s vozidlem a podporující výměnu informací mezi zařízením na pozemní komunikaci (RSE) nebo s centrální komunikační jednotkou; je složeno z palubní jednotky ve vozidle (OBU) a dalších subjednotek, jejichž přítomnost musí být povinná při provádění transakce

3.17 palubní jednotka *(on–board unit)* minimální komponenta palubního zařízení (OBE), jejíž funkce vždy zahrnuje minimálně DSRC rozhraní

3.18 profil *(profile)* množina jedné nebo více základních norem a/nebo profilů ISP, a kde je to vhodné, identifikace vybraných tříd, shodných podmnožin, volitelných možností a parametrů těchto základních norem nebo profilů ISP nezbytných pro splnění konkrétní funkce [ISO/IEC TR 10000]

3.19 zařízení na pozemní komunikaci; zařízení na straně infrastruktury *(roadside equipment)* pevně umístěné zařízení na silniční síti za účelem komunikace a přenosu dat na OBE projíždějících vozidel

4 Zkratky

Kapitola 4 uvádí 28 zkratek.

5 Shoda

5.1 Požadavky na palubní jednotku OBU

Článek 5.1 obsahuje veškeré požadavky na OBU, a to v následujícím členění: požadavky na DSRC (článek 5.1.1), DSRC L7 a funkce EFC (článek 5.1.2), požadavky na data (článek 5.1.3), požadavky na bezpečnost (článek 5.1.4) a požadavky na transakci (článek 5.1.5).

Příklad požadavků na OBU (čl. 5.1:

Palubní jednotka OBU se musí shodovat s:

Profily DSRC P0 / P1 L1–B podle EN 13372

nebo

Profily DSRC P0 / P1 L1–A podle EN 13372 se směšovacím ziskem, který je omezen na maximální hodnotu 10 dB (Parametr U12b = 10dB) a mezním výkonem minimálně -60dBm (Parametr D12 = -60dBm).

5.2 Požadavky na zařízení na pozemní komunikaci (RSE)

Článek 5.2 obsahuje veškeré požadavky na RSE, a to v obdobném členění jako požadavky na OBU: požadavky na DSRC (článek 5.2.1), DSRC L7 a funkce EFC (článek 5.2.2), požadavky na data (článek 5.2.3), požadavky na bezpečnost (článek 5.2.4) a požadavky na transakci (článek 5.2.5).

Příloha A (informativní) Specifikace dat

Tato příloha obsahuje podrobný seznam (normativní) o způsobu specifikace a použití datových prvků. Uvádí smluvní data (tab. A.1), data vozidla (tab. A.2, viz ukázka) a zařízení a přijetí dat (tab. A.3).

Tabulka A.2 – Data vozidla

Identifikátor Atributu / Název Datový prvek	Definice & poznámky	Použití	Délka v oktetech
VOZIDLO	Informace náležící k identifikaci a charakteristikám vozidla		
16 / SPZ vozidla SPZ vozidla	Požadovaná SPZ vozidla	Používání podle EN ISO 14906. Požadovaná SPZ vozidla, délka SPZ je pevně stanovena na 10 oktetů. SPZ, která je kratší než 10 čísel, je doplněna čísly nula tak, aby se dosáhlo celkové délky 10 čísel. Příklad : SE, LatinAlphabethNo1, OCD560 Kód země = SE = 1010010000'B Indikátor abecedy = LatinAlphabethNo1 = 000000'B determinant délky = 10 octets = 00001010'B SPZ = OCD560 = 4F 43 44 35 36 30 00 00 00 00'H	13
17/ Třída vozidla Třída vozidla	Konkrétní informace poskytovatele služby náležící vozidlu.	Substruktura třídy vozidla TCCC LLLL, kde T (indikátor přívěsu) : 0'B = bez přívěsu, také se používá defaultní hodnota 1'B = s přívěsem CCC (Evropské Prohlášení o dohodě MoU) : 000'B = Skupina 0 – Motocykly (UNECE třída L) 001'B = Skupina 1 – Malá osobní vozidla (UNECE třída M_1) 010'B = Skupina 2 – Lehká nákladní vozidla (UNECE třída N_1) 011'B = Skupina 3 – Velká osobní vozidla (UNECE třída M_2, M_3) 100'B = Skupina 4 – Těžká nákladní vozidla (UNECE třída N_2, N_3) 101'B = nepoužívá se 110'B = nepoužívá se 111'B = Skupina 7 – Jiná vozidla LLLL (Třídy místních vozidel): přidělení hodnoty podle lokálního schématu	1

Příloha B (normativní) Šifrovací výpočty

Tato příloha ilustruje popis šifrovacích mechanismů a jejich výpočtů požadovaných touto normou.

Příklad autentizátoru atributu:

a) Nechť je AuK autentizačním klíčem pro OBU dané generace k, odkazovaného pomocí KeyRef v požadavku GET_STAMPED.

b) Nechť je M seznamem atributů v odpovědi na GET_STAMPED řetězeném oktetovým řetězcem obsahujícím RndRSE zaslaným v požadavku GET_STAMPED. RndRSE musí obsahovat čas relace.

c) Rozděl M na 8–oktetové bloky D_1 (oktety 1 až 8), D_2 (oktety 9 až 16),...., D_{n-1} (oktety 8(n–1) až 8n)

d) Podle [ISO/IEC 9797–1] MAC algoritmus 1 musejí být zbývající bity ponechány k ověření. Napravo od těchto se musí připojit bity nulové hodnoty tak, že poslední 8–oktet blok vyústí v D_n.

e) První blok D_1 musí být operátorem jazyka XOR upraven s počáteční hodnotou 00000000 a tento výsledek musí být vstupem I_1 prvního kroku:

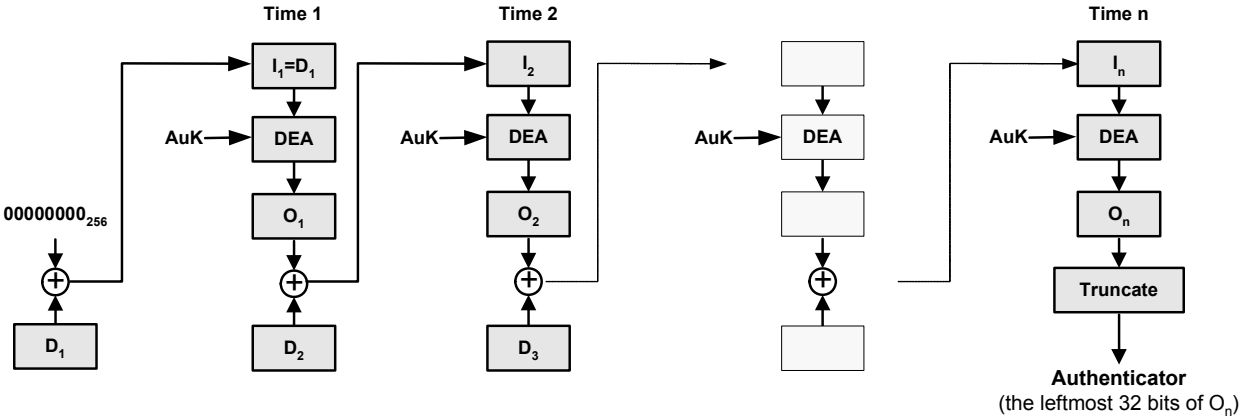
I_1= [00000000] XOR [D_1]

f) První krok: první blok I_1=D_1 se musí zašifrovat pomocí AuK:

O_1= e[AuK](I_1)

g) Výstup O_1 musí být operátorem jazyka XOR upraven s D_2 a tento výsledek musí být vstupem I_2 dalšího kroku:

I_2= [O_1] XOR [D_2]…



Truncate = zkrátit

The leftmost 32 bits of O_3 = levých krajních 32 bitů O_3

Obrázek B.1 – Algoritmus pro autentizaci atributů

Příloha C (normativní) Formulář prohlášení o shodě implementace (ICS)

Pro hodnocení shody určité implementace je nezbytné mít prohlášení, které schopnosti a možnosti byly implementovány pro telekomunikační specifikaci. Takové prohlášení se nazývá prohlášení o shodě implementace ICS *(Implementation conformance statement)*. Tato příloha uvádí formuláře ICS, které vyplní dodavatelé zařízení.

Pokud dodavatelé výrobku tvrdí, že jsou ve shodě s touto normou, musí být aktuální formulář ICS, jež má dodavatel vyplnit, technicky ekvivalentní k textu formuláře ICS obsaženého v této příloze a musí zachovat číslování/nazývání a pořadí položek tohoto formuláře.

Formuláře uváděné v této příloze musí být vyhotoveny dodavatelem IUT (IUT = položka, která je předmětem zkoušky, např. OBU nebo RSE). Formulář ICS je rozdělen na ustanovení pro následující kategorie informací:

– Pokyny pro vyplnění formuláře ICS;
– Identifikace implementace;
– Identifikace protokolu;
– Globální prohlášení o shodě;
– Tabulky formuláře ICS.

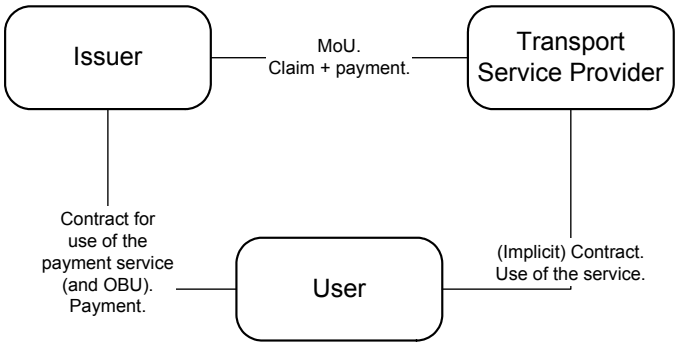
Norma uvádí v příloze C celkem 44 tabulek pro prohlášení o shodě.

Příloha D (informativní) Přehled služby EFC

D.1 Referenční model služby EFC

Služba EFC není podrobně definována v žádné normě. Obecně se předpokládá, že operátoři používající normy EFC mohou definovat aktuální službu. Nicméně použití této normy vyžaduje jistou základní znalost služby EFC; např. že obsahuje některé konkrétní prvky a drží se některých základních principů. Proto je níže uveden jednoduchý referenční model služby EFC. Tento referenční model udává definici minimální společné služby, která se požaduje pro vlastní použití této normy. Tento referenční model je tudíž velmi zjednodušený ve srovnání s obchodními modely používanými v projektech interoperability jako jsou CARDME, CESARE a PISTA nebo obdobné národní projekty.

Základní struktura odpovědností v rámci služby Interoperabilní EFC je ukázána na následujícím obrázku. Obrázek definuje základní entity, organizace a role.



Legenda

issuer	vydavatel	user	uživatel
transport service provider	poskytovatel dopravních služeb		
MoU Claim + payment	Prohlášení o dohodě (nárok + platba)		
Contract for use…	Smlouva na použití placené služby (a OBU). Platba		
(Implicit) contract…	(Implicitně) smlouva. využití služby.		

Obrázek D.1 – Referenční model pro základní aktivní členy v interoperabilní EFC (termíny se mohou mezi projekty lišit)

Příloha E (informativní) Příklady šifrovacích výpočtů

Tato příloha uvádí kryptografický (šifrovací) mechanismus definovaný v kapitole 5 a příloze B pomocí několika numerických příkladů.

Příloha F (informativní) Bezpečnostní pokyny

Tato příloha uvádí pozadí a pohnutky k bezpečnostním znakům uváděným v této normě.

Příloha G (informativní) Management mezi vrstvami

V této normě nejsou žádné požadavky na management mezi vrstvami (např. tabulky stavových přechodů, apod.), neboť neexistují základní normy definující tyto aspekty. Proto tato norma aplikačního profilu nemůže klást požadavky na management mezi vrstvami pomocí formátu ISP. Tato informativní příloha je sestavena jako řada pokynů a seznam způsobů provedení managementu mezi vrstvami.

Příloha H (informativní) Klasifikační data vozidla

Definované datové atributy vozidel nejsou určeny jako povinné pro všechny OBU všech typů vozidel. Naopak je řešení postaveno na různých třídách vozidel (typech), které vyžadují různá nastavení dat pro implementaci v OBU. Primárně jsou definovány dvě různé třídy vozidel;

a) Soukromá vozidla, která patří do předdefinované třídy, a nevyžadují, aby byla podrobná data vozidla uložena v OBU.

b) Těžká vozidla (nad 3,5 tuny); která vyžadují, aby byla podrobná data vozidla uložena v OBU (pro implementaci schémat zpoplatnění těžkých nákladních vozidel (HGV)).

Vozidla se dělí na několik základních skupin (viz úplná podoba tabulky 10):

Tabulka 1 – Navržené evropské skupiny vozidel (vzato ze zprávy expertní skupiny EG2)

Skupina	Popis	Charakteristiky	Třída UNECE
0	Motocykly	2 nebo 3 kola	L
1	Malá osobní vozidla	sedadla ≤ 8 + řidič	M_1
2	Lehká nákladní vozidla	váha ≤ 3,5 t	N_1
3	Velká osobní vozidla	sedadla > 8 + řidič	M_2, M_3
4	Těžká nákladní vozidla	váha > 3,5 t	N_2, N_3

5	Nepoužívá se		
6	Nepoužívá se		
7	Jiná vozidla		

Příloha I (informativní) Použití této normy pro jiné transakce DSRC

Tato norma definuje aplikační profil pouze pro jeden typ transakcí; Transakce zpoplatnění EFC pomocí platby na centrální účet. Nicméně protože je funkčnost v RSE a OBU modulární, je možné definovat jiná schémata transakcí pro OBU a RSE, která jsou ve shodě s touto normou. Tato příloha uvádí stručné pokyny, jak lze tuto normu použít jako základ pro jiná schémata transakcí (např. transakce dohledu).

Příloha J (informativní) Montážní pokyny pro OBE

Pro možnost interoperability mezi zařízeními od různých výrobců je nezbytné stanovit nejen požadavky na transakce, ale i dostatečně definovat geometrické aspekty komunikace. Tato příloha obsahuje pokyny pro montáž týkající se polohy a orientace OBE, což umožní RSE, aby byla navržena a instalována pro dosažení interoperability. Je důležité, aby všechny RSE měly takový design, který by umožnil zacházet se všemi OBE včetně verzí, které splňují minimální požadavky uvedené níže.