EXTRAKT z české technické normy

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

35.240.60

Dopravní telematika – Elektronický výběr poplatků (EFC) – Definice rozhraní pro palubní účet používající platební kartu ICC

ČSN P CEN TS 25110

01 8387

Platí od 2009 (bude doplněno)

37 stran

Úvod

Existují dva platební systémy EFC. Jedním je systém centrálního účtu používající palubní jednotky OBU, druhý je systém palubního účtu používající média, jako je karta s integrovaným obvodem (ICC).

Karta ICC je běžně používána jako platební karta ve veřejné přepravě osob, v metru nebo v autobuse, a jako karta s elektronickými platebními prostředky pro běžné platby, jako je kreditní karta nebo bankovní karta. Předpokládá se, že se karta ICC bude používat pro účely plateb EFC podle globálních trendů, neboť je dostatečně vhodná a flexibilní pro platící osobu. Navíc vývoj mobilního telefonu s integrovanými funkcemi platební karty, nazývaný také „mobilní elektronická peněženka“, je v některých zemích běžně používán pro veřejnou dopravu nebo maloobchodní nákupy jako platební prostředek.

Cílem této normy je klasifikace modelů přenosu dat založených na provozních požadavcích a definování specifického přístupového rozhraní karty ICC na účet palubní jednotky používající ICC pro každý model. Dále tato norma v příloze uvádí praktické příklady transakce, které jsou bezproblémově přijatelné pro provozovatele mýtného, jenž hodlá zavést nový systém mýtného.

Užití

Tato norma poskytuje běžnou technickou platformu provozních požadavků pro účet palubní jednotky používající ICC a praktické příklady tohoto účtu, které jsou v současné době používány nebo plánovány v několika zemích. Každý operátor mýtného může zavést svou vlastní specifikaci volbou jednoho příkladu z modelů uvedených v této normě (jako své vlastní nástroje (tool box)), aby splnil příslušné požadavky.

Souvisící normy

Tuto normu je nutno číst v návaznosti na hlavní specifikaci EFC EN ISO 14906, zkušební specifikace CEN ISO/TS 14907-1 a 2, specifikaci systému bezpečnosti CEN TS 17574 a aplikační vrstvy ISO 15628.

1 Předmět normy

Tato mezinárodní norma definuje modely datového přenosu mezi zařízením na pozemní komunikaci RSE a platební kartou ICC a popisy rozhraní mezi RSE a OBE pro palubní účet používající ICC. Dále uvádí užitečné příklady rozhraní a transakce, aktuálně používaných v několika zemích.

Předmět této normy zahrnuje:

– Modely datových přenosů mezi RSE a ICC, které odpovídají kategorizovaným provozním požadavkům a mechanismus datového přenosu pro každý model;

– definici rozhraní mezi RSE a OBE založenou na každém modelu datového přenosu.

Definice rozhraní pro každý model zahrnuje:

– Funkční konfiguraci;

– definice příkazů RSE pro přístup ICC;

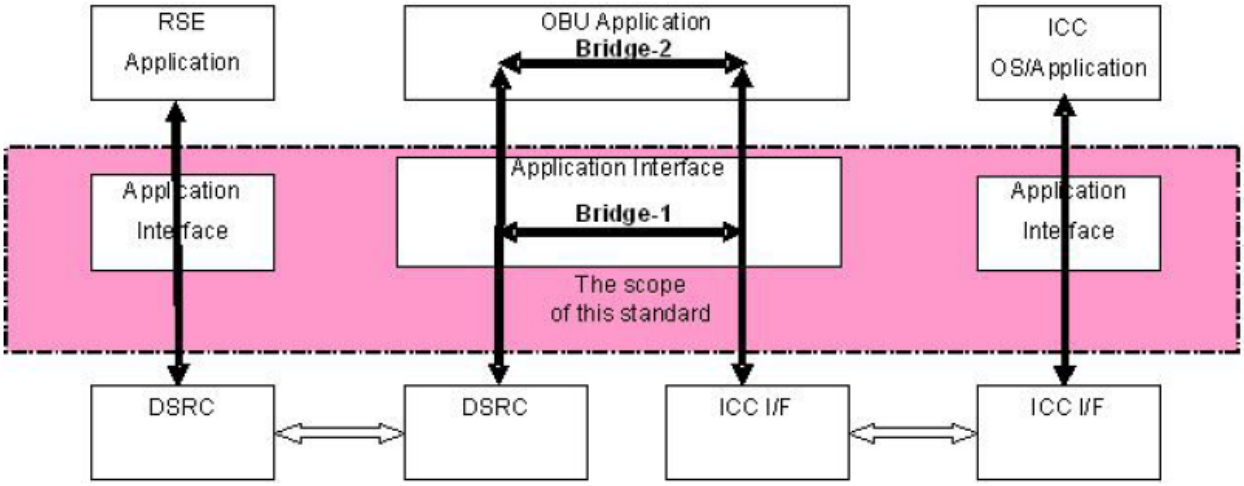
– definici datového formátu a datových prvků příkazů RSE;

– příklad transakce pro každý model uvedený v příloze.

Popisy této normy se zaměřují na rozhraní mezi RSE a OBU pro přístup na ICC.

Existují dva typy virtuálního mostu vytvořeného v OBU. Jedním je Most-1 (Bridge-1), na kterém je příkaz RSE zaslaný z RSE rozložen a příkaz přístupu na ICC obsažený v části APDU příkazu RSE je přenesen na ICC I/F pro přístup na ICC. Druhým je Most-2 (Bridge-2), na kterém je příkaz RSE zaslaný z RSU transformován na příkaz přístupu na ICC a je přenesen na ICC I/F pro přístup na ICC.

Most-1 odpovídá transparentnímu typu a typu vyrovnávací paměti (buffering type) definovaný touto normou a Most-2 odpovídá paměťovému typu (caching type).



Obrázek 4 – Předmět této normy

3 Termíny a definice

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) [EN ISO 14906]

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.

3.13 palubní jednotka *(on–board unit)* minimální komponenta palubního zařízení (OBE), jejíž funkce vždy zahrnuje minimálně DSRC rozhraní [EN ISO 14906]

3.14 zařízení na pozemní komunikaci *(roadside equipment)* pevně umístěné zařízení na silniční síti za účelem komunikace a přenosu dat na OBE projíždějících vozidel [EN ISO 14906]

3.16 základ služby (komunikace) *(service primitive (communication))* základní komunikační služba poskytovaná protokolem aplikační vrstvy aplikačnímu procesu [EN ISO 14906]

POZNÁMKA Spuštění základní služby aplikačním procesem implicitně vyvolává využití nabízených služeb nižších vrstev protokolu.

3.18 relace *(session)* výměna informací a interakce vzniklá na dané stanici EFC, která probíhá mezi zařízením v blízkosti pozemní komunikace a uživatelem/vozidlem [EN ISO 14906]

3.19 transakce *(transaction)* kompletní výměna informací mezi zařízením v blízkosti pozemní komunikace (RSE) a palubním zařízením (OBE) nutná pro dokončení operace EFC prostřednictvím DSRC [EN ISO 14906]

4 Zkratky

Kapitola 4 uvádí 19 zkratek popisujících zabezpečení čipových karet.

4.1 AID Application identifier – identifikátor aplikace

4.13 MAC Medium access control – jedinečný identifikátor síťového zařízení

4.14 ICC Integrated circuit(s) card – karta s integrovaným obvodem

4.18 SAM Secure application module – zabezpečovací aplikační modul

5 Požadavky na účet palubní jednotky

5.1 Požadavky na provoz účtu palubní jednotky

Hlavními faktory provozních požadavků pro EFC jsou rychlost vozidla a úroveň zabezpečení informací a oba požadavky významně ovlivňují základní návrh systému EFC.

5.2 Druh platební karty ICC

Platební karta ICC používaná pro účet palubní jednotky se klasifikuje na

– kontaktní druh karty ICC

– bezkontaktní druh karty ICC

– hybridní druh karty ICC

Kontaktní druh platební karty ICC založený na souboru norem ISO/IEC 7816 byl vyvinut a je používán pro účely finančního sektoru jako bankovní a kreditní karty a bez kontaktní druh karty ICC založený na souboru norem ISO/IEC 14443 nebo ISO/IEC 18092 byl vyvinut a je používán pro účely veřejné přepravy osob, ve vlacích, autobusech a metru. Hybridní druh karty ICC má obě funkce definované souborem norem ISO/IEC 7816 a ISO/IEC 14443 nebo také ISO/IEC 18092 a je používán jako multifunkční karta, jako karta EFC a karta veřejné přepravy osob.

5.3 Požadavky na interoperabilitu ICC

Z důvodu bezpečnosti a přenositelnosti karty se po kartě ICC potenciálně požaduje interoperabilita s jinými službami jako prostředek k běžným platbám. Předpokládá se, že požadovaná úroveň interoperability platební karty ICC se bude pohybovat v těchto třech úrovních:

– Úroveň 1: Interoperabilita v rámci skupiny smluvních provozovatelů mýtného;

– Úroveň 2: Interoperabilita rozšířená na aplikace veřejné přepravy osob;

– Úroveň 3: Interoperabilita rozšířená dále na maloobchodní aplikace.

6 Model datového přenosu

6.1 Všeobecně

Existují tři typy modelu datového přenosu pro účet palubní jednotky používající kartu ICC, aby odpovídal provozním požadavkům uvedeným v kapitole 5.

– **Transparentní typ** (čl. 6.1.1), kde se příkazová data karty ICC přenesou přímo z RSE na kartu ICC přes OBU. OBU uloží příkazová data karty ICC a dočasně i odpovědní data do vyrovnávací paměti.

– **Paměťový typ (caching)** (čl. 6.1.2), kde jsou data související s EFC čtena z karty ICC při prezentaci a uložena v zabezpečovacím aplikačním modulu SAM OBU. V komunikaci DSRC jsou data související s EFC uložena v SAM a přenesena do RSE.

– **Typ s vyrovnávací pamětí (buffering)** (čl. 6.1.3), kde jsou data související s EFC, která jsou omezena na data, která nejsou citlivá, čtena z karty ICC při prezentaci a uložena ve vyrovnávací paměti OBU. V komunikaci DSRC jsou data související s EFC ve vyrovnávací paměti přenesena do RSE.

6.2 Symboly

Článek popisuje symboly uváděné v mechanismu datového přenosu každého modelu.

6.3 Transparentní typ

6.3.1 Obecný popis

V tomto modelu závisí maximální rychlost vozidla na rychlosti datového přenosu mezi platební kartou ICC a OBU, takže vozidlo musí zastavit a nebo projíždět pomalu pod anténou RSE v případě, že se použije běžný kontaktní druh karty ICC. Základním znakem transparentního typu je jednoduchá OBU,

která má omezenou bezpečnostní paměť v OBU, a výkon se zlepší podle vývoje karet ICC s vysokorychlostním přenosem dat.

6.3.2 Proces datového přenosu

Článek popisuje proces datového přenosu a je doprovázen ilustrativním obrázkem.

6.4 Paměťový typ (caching)

6.4.1 Obecný popis

V tomto modelu OBU čte datové sety z karty ICC a ukládá je do zabezpečené paměti v OBU, po vložení karty ICC do OBU a ukončení následného procesu autentizace. Základním znakem tohoto typu je, že vysoká rychlost výměny dat mezi RSE a OBU se provede i přesto, že se použije ICC s pomalou přenosovou rychlostí. S paměťovým typem je zvýšena maximální rychlost vozidla do výkonu DSRC spojení bez ohledu na přenosovou rychlost karty ICC.

6.4.2 Proces datového přenosu

Článek popisuje proces datového přenosu a je doprovázen ilustrativním obrázkem.

6.5 Typ s vyrovnávací pamětí (buffering)

6.5.1 Obecný popis

Typ s vyrovnávací pamětí má oba základní znaky transparentního typu a paměťového typu, nicméně datové sety uložené v kartě ICC jsou omezeny na data, která nejsou citlivá, aby nemohlo dojít k jejich falšování a nebo prozrazení. V tomto typu je metoda datového přenosu stejná jako u paměťového typu a datové sety jsou čteny a uloženy ve vyrovnávací paměti OBU poté, co byla karta ICC do OBU vložena. Datové sety uložené ve vyrovnávací paměti jsou přeneseny do RSE během čtecí sekvence DSRC. V případě zápisu jsou datové sety RSE přeneseny do OBU a uloženy ve vyrovnávací paměti OBU a poté přeneseny do karty ICC.

6.5.2 Proces datového přenosu

Článek popisuje proces datového přenosu a je doprovázen ilustrativním obrázkem.

7 Definice rozhraní pro přístup na platební kartu ICC

7.1 Transparentní typ

Článek 7.1.1 popisuje funkční konfiguraci transparentního typu a článek 7.1.2 příkaz a odpověď mezi RSE a OBU doplněný tabelárním přehledem.

7.2 Paměťový typ

Obdobně článek 7.1.2 popisuje funkční konfiguraci paměťového typu a článek 7.2.2 příkaz a odpověď mezi RSE a OBU doplněný tabelárním přehledem.

7.3 Typ s vyrovnávací pamětí

Obdobně článek 7.1.3 popisuje funkční konfiguraci typu s vyrovnávací pamětí a článek 7.3.2 příkaz a odpověď mezi RSE a OBU doplněný tabelárním přehledem.

Příloha A (informativní) Příklad metody přístupu na platební kartu ICC

A.1 Model transparentního typu

A.1.1 Model 1 transparentního typu (pro předplacené platby)

A.1.1.1 Všeobecně

Jako příklad transparentního typu, model 1, je přístup na kartu ICC pomocí funkce přenosového kanálu definované v ISO 14906.

– Příkaz: Transfer_channel definovaný jako ActionType=8

– AID: EFC aplikace definovaná jako AID=1 v ISO 15628

– ID kanálu: karta ICC definovaná jako ChannelID=icc(3) v ISO 14906

– Typ ICC: bezkontaktní druh předplacené karty ICC

A.1.1.2 Definice příkazu RSE

Tento článek uvádí příklady příkazu a odpovědi v tabelárním přehledu.

A.1.1.3 Transakce

Tento článek uvádí příklad komunikace při transakci, při vjezdu a při výjezdu ze zóny.

A.1.2 Model 2 transparentního typu (pro zpětné platby)

A.1.2.1 Všeobecně

Jako příklad transparentního typu, model 2, je metoda přístupu na kartu ICC pomocí „Základního aplikačního rozhraní DSRC“ ustaveného ITS Fórem v Japonsku.

„Základní aplikační rozhraní DSRC“ je ustaveno tak, aby poskytovalo Vícečetné informační služby jako jsou dopravní informace a informace o stavu vozovky, informace pro cestující, parkovací informace apod. s identifikačním ID aplikace jako AID=18 registrované v ISO 15628. Dále k těmto hlavním informačním službám je přístup na kartu ICC definován pro aplikaci platby za parkování.

A.1.2.2 Definice příkazu RSE

Tento článek uvádí příklady příkazu a odpovědi v textové formě a tabelárním přehledu.

A.1.2.3 Transakce

A.1.2.3.1 Parkovací systém

Tento článek uvádí příklad komunikace při transakci, při vjezdu a při výjezdu ze zóny:

– (1) Jednoduchého systému (Metoda spojení s centrem (Center chaining method)).

V tomto systému má být poplatek za parkování zaplacen kreditní kartou, jejíž číslo je registrováno v centrálním systému, ve kterém je číslo kreditní karty propojeno s číslem členství. Pro smluvní členství a platbu je nutné číslo kreditní karty nejdříve zaregistrovat v centrálním systému.

– 2) Komplexní systém (Přímá metoda (Direct method))

V tomto systému má být poplatek za parkování zaplacen kreditní kartou, jejíž číslo je přečteno přímo z kreditu karty ICC.

A.2 Model paměťového typu

A.2.1 Všeobecně

Jako příklad modelu paměťového typu je popsána metoda přístupu na kartu ICC používaná v systému elektronického vybírání mýtného (ETC) v Japonsku. V japonském ETC je distribuce OBU založena na maloobchodním prodeji v prodejnách aut a jakýkoliv výrobce se může trhu s OBU zúčastnit, pokud získá schválení typu od zkušebního institutu. Proto se požaduje vysokoúrovňové zabezpečení dat pro platební kartu ICC a příslušná data výběru mýtného uložená v OBU a schválení výrobci OBU musí vybavit OBU SAM od certifikovaného výrobce SAM věrohodnou třetí stranou.

A.2.2 Definice příkazu RSE

Tento článek uvádí příklady příkazu a odpovědi v textové formě a tabelárním přehledu.

A.2.3 Transakce

Tento článek uvádí příklad komunikace při transakci, při vjezdu a při výjezdu ze zóny.

Článek A.2.3.1 uvádí schéma paušální platby ETC (Otevřený systém) a kreditní platby.

Článek A.2.3.2 uvádí schéma platby ETC podle vzdálenosti (Uzavřený systém) a kreditní platby.

A.3 Model typu s vyrovnávací pamětí

A.3.1 Všeobecně

Jako příklad modelu typu s vyrovnávací pamětí je popsána metoda přístupu na kartu ICC používaná v systému elektronického vybírání mýtného (ETC) v Koreji. V korejském ETC je používán hybridní druh karty ICC nejen pro účely ETC, ale také pro systém Touch & Go, kde řidič může projet zpoplatněným pruhem při dotyku své platební karty se čtečkou na pozemní komunikaci.

– Definice příkazu: definována korejskými normami pro účely výběru mýtného ETC

– Příkaz: Initialize, Action(Debit, Set-secure), Get and Release definované v ISO 14906
– AID: Elektronické vybírání mýtného(EFC) definovaná jako AID=1 v ISO 15628
– Druh ICC: hybridní druh karty ICC s předplacenou platbou

A.3.2 Definice příkazu RSE

Tento článek uvádí příklady příkazu a odpovědi v textové formě a tabelárním přehledu.

A.3.3 Transakce

Tento článek uvádí příklad komunikace při transakci, při vjezdu a při výjezdu ze zóny.

Příloha B (informativní) Interoperabilní vztahy s jinými sektory

Příloha uvádí dva obrázky ilustrující vztahy provozní interoperability. Obrázek B.1 znázorňuje vztah provozní interoperability, kde se požaduje, aby platební karty ICC vydané pro účely EFC byly použity pro aplikace veřejné přepravy osob a/nebo maloobchodní aplikace. Naopak obrázek B.2 znázorňuje ostatní vztahy provozní interoperability, kde se požaduje, aby karty ICC vydané pro účely veřejné přepravy osob, které se považují za přenosné elektronické platební médium nebo maloobchodní platby, byly použity pro účely EFC.