Jindřich Borka[1]

Bezkontaktní technologie v odbavovacích systémech

Klíčová slova: *BackOffice, bezkontaktní čipová karta, FrontOffice, jízdní doklad, odbavovací systém, Nařízení vlády č. 295/2010 Sb., NFC, technický nosič, RFID, Zákon o veřejných službách v přepravě cestujících*

Odbavení cestujících, odbavovací systém – úvod a obecná definice

Odbavení cestujících z hlediska procesního

Pod pojmem odbavení cestujících si lze představit na první pohled poměrně jednoduchý proces „prodeje jízdenky cestujícímu a její následné kontroly v dopravním prostředku“. Takový popis se však jeví jako nedostatečný, uvědomíme-li si, že vlastnímu prodeji jízdenky cosi předchází, že vlastní prodej s sebou nese práci s informačními systémy, výběr vhodného spojení, rezervace, validaci jízdního dokladu atd.

Z širšího pohledu lze definovat odbavení cestujících jako množinu procesů, které probíhají nad odbavovacím systémem. Množina procesů odbavení cestujících potom sestává z:

- Příprava tarifu, ceníky, jízdní řády apod.,
- výběru vhodného spojení (= informování cestujících před cestou),
- **zadání požadavku na jízdní doklad, reservaci, lůžko/lehátko atp.,**
- **platby,**
- **výdeje jízdního dokladu,**
- **validace jízdního dokladu,**
- informování cestujících v průběhu cesty,
- zpracování dat z prodeje.

Procesy odbavení probíhají různě v závislosti na příslušném tarifu, použitém způsobu platby a fyzickém nosiči jízdního dokladu. Fyzický nosič jízdního dokladu, v našem případě umožňující bezkontaktní zápis a čtení jízdního dokladu, je předmětem další části příspěvku.

[1] Jindřich BORKA ing., nar. 1974 v Praze, ČVUT FD v Praze, obor automatizace v dopravě a telekomunikacích, pracoviště ČD IS a.s., odd. vývoj Praha, systémový architekt, odbavovací systémy a systémy pro podporu provozu osobní dopravy, studující doktorandského studia na ČVUT FD Ústavu řídící techniky a telematiky.

Odbavení cestujících z hlediska systémového

Odbavovací systém je v podstatě systém, který pokrývá procesy odbavení a je tvořen jednotlivými prvky odbavovacího systému a vazbami mezi nimi. Základem odbavovacího systému je obecně FrontOffice[2], BackOffice[3], prvky komunikační infrastruktury, prvek nosiče jízdního dokladu a rozhraní. Do okolí odbavovacího sytému lze zařadit například systémy rozúčtování tržeb, věrnostní systémy, systémy pro informování cestujících atp.

Právní rámec bezkontaktního odbavení

Pro ucelený pohled na problematiku odbavení cestujících i odbavovací systémy uvádím základní přehled právních norem, kterými je tato oblast právně pokryta.

Problematiku odbavování cestujících částečně pokrývá Zákon č. 266/1994 Sb., o dráhách, podrobněji jsou pak pravidla upravena zákonem 194/2010 Sb. - Zákon o veřejných službách v přepravě cestujících a o změně dalších zákonů.
Technické podmínky odbavení cestujících elektronickými jízdními doklady upravuje Nařízení vlády č. 295/2010 Sb., ze dne 20. října 2010 o stanovení požadavků a postupů pro zajištění propojitelnosti elektronických systémů plateb a odbavení cestujících a dále Příloha č. 1 k nařízení vlády č. 295/2010 Sb.

„Toto nařízení stanoví požadavky a postupy pro zajištění technické a provozní propojitelnosti elektronických systémů plateb a odbavení cestujících a jejich zařízení a technologií při zajišťování dopravní obslužnosti (dále jen "systém elektronického odbavení cestujících"), provozovaných státem, krajem, obcí nebo jimi pověřenou osobou (dále jen "provozovatel systému elektronického odbavení cestujících"). [1]

Nařízení dále v Příloze č. 2 upravuje požadavky na technické řešení systému elektronického odbavení cestujících, ve které stanovuje podmínky, za kterých jsou požadavky splněny.

Příloha č. 2. Nařízení dále vyčítá požadavky na „technický nosič dat“ (= nosič jízdního dokladu). Pro další popis zde uváděné problematiky si dovoluji Přílohu 2. uvést.

„*Požadavky na technický nosič dat jsou splněny za předpokladu, že technický nosič má jednoznačný identifikátor a technologie technického nosiče dat umožňuje:*

a) *řízení přístupu k jednotlivým aplikacím pro účely čtení i zápisu,*
b) *oddělování datových prostorů v paměti tak, aby bylo zajištěno souběžné a nezávislé ukládání, mazání, a změna aplikací a jejich datového obsahu pro různé systémy elektronického odbavení cestujících, a to i v průběhu pozdějšího používání technického nosiče dat cestujícím,*
c) *ukládání aplikací a jejich datového obsahu tvořeného údaji o jízdním dokladu, příplatku nebo místence nezbytnými pro dopravní využití,*

[2] Pro odbavovací systém ČD jsou to typicky pokladny UNIPOK, prodejní automaty jízdenek, přenosné osobní pokladny POP, web eShopu
[3] Centrální systémy. V odbavovacím systému ČD jsou to reservační systém, Archiv primárních dat, CardManagement, systémy rozúčtování – OPT – Odúčtovna přepravních tržeb atp.

d) zabezpečení technického nosiče dat, jednotlivých aplikací na něm uložených a jejich datového obsahu proti neoprávněnému čtení, mazání a neoprávněné změně nepovolanou osobou,

e) disponování vnitřními bezpečnostními prvky pro šifrování uložených dat a řízení přístupu k aplikacím pomocí kryptografických klíčů,

f) zavedení dalších bezpečnostních prvků s využitím prostředků, které jsou na vnitřních bezpečnostních prvcích technického nosiče dat nezávislé,

g) obnovování kryptografických klíčů použitých pro ochranu aplikací a jejich datového obsahu uložených na technickém nosiči dat za provozu a

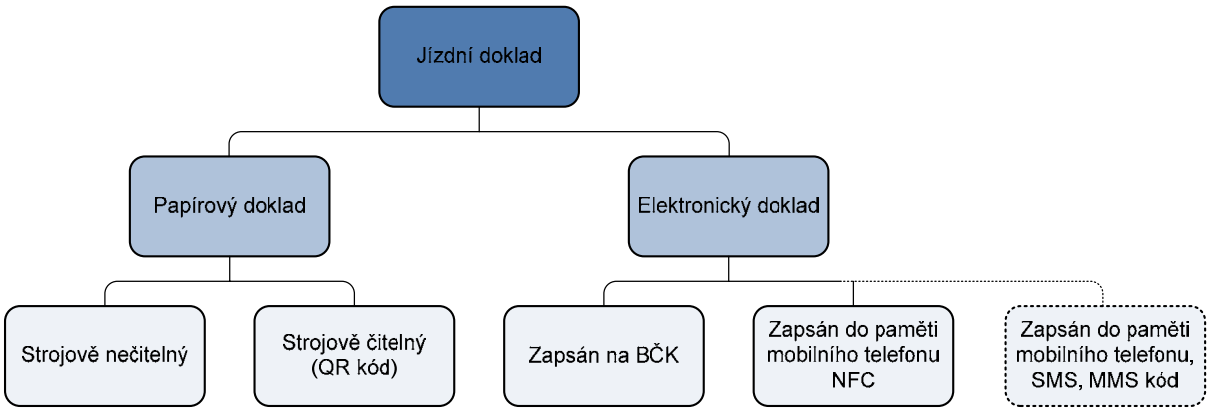
h) uložení aplikace využitelné k uchovávání:

1. *jízdního dokladu, příplatku nebo místenky,*
2. *předplatného jízdného v případě bezkontaktní čipové technologie.“* [2]

Druhy jízdních dokladů podle nosiče

Jízdní doklad může být zapsán na papírové resp. elektronické médium v podobě přímo čitelné a (nebo) strojově čitelné. Kombinací nosiče jízdního dokladu a jízdního dokladu potom dostaneme:

- Papírový jízdní doklad – informace jsou vytištěny na papírový nosič – jízdenku, informace jsou v podobě přímo čitelné (resp. strojově čitelné, čárové kódy, QR kódy, Aztécké kódy atp.). Jízdní doklad je zabezpečen proti zneužití fysicky- vodotiskem, giloši, hologramem. Informace uložená v QR kódu resp. Aztéckém kódu je zabezpečena kontrolními součty a šifrováním.
- Elektronický jízdní doklad – informace (elektronická jízdenka) jsou uloženy v digitální podobě na vhodném paměťovém médiu, přičemž při výdeji je možno vytisknout daňový doklad. Nosičem je potom:
  - bezkontaktní čipová karta (BČK), uložená informace je zabezpečena zašifrováním kryptografickými klíči a řízením přístupu do aplikací karty,
  - mobilní telefon, který je vybaven NFC rozhraním, uložená informace je zabezpečena zašifrováním kryptografickými klíči a řízením přístupu do aplikace uložené přímo v telefonu, nebo v SIM telefonu,
  - paměť mobilního telefonu, SMS/MMS kód elektronické jízdenky, uložená informace je zabezpečena kontrolními součty/zašifrováním, nebo i prostřednictvím webové aplikace (Back-office) provozovatele služby.



Obrázek 1 - Druhy jízdních dokladů podle typu nosiče[4]

Bezkontaktní odbavení

Principem bezkontaktního odbavení je čtení/zápis jízdního dokladu z/na nosič jízdního dokladu bez fysického kontaktu nosiče se zařízením určeným ke čtení/zápisu. Zvláštní způsob bezkontaktního odbavení je i zápis jízdního dokladu do čárového resp. QR kódu. I když je tento kód fysicky natištěn na nosiči, umožňuje bezkontaktní čtení čtečkami čárových kódů.

Bezkontaktní čipová karta

Bezkontaktní čipová karta je základním prvkem bezkontaktního způsobu odbavení. Bezkontaktní čipová karta sestává z čipu s bezkontaktním rozhraním - anténou a příslušnými obvody a plastovým tělem. V plastovém těle, které nemusí být bezpodmínečně známého formátu bankovní karty, je pak čip s rozhraním zalisován.

Bezkontaktní rozhraní čipu je tvořeno cívkou/anténou. Anténa je tvořena definovaným počtem a velikostí závitů. Velikost antény a počet závitů určuje kmitočet, na kterém má bezkontaktní čipová karta pracovat.

Po přiblížení bezkontaktní čipové karty do elektromagnetického pole čtečky o příslušném kmitočtu, dochází k navázání komunikace karty se čtečkou.

Typů bezkontaktních čipových karet je velké množství. Může se jednat o nejprostší tzv. RFID (z Angl. Radio Frequency Identification – identifikace na rádiové frekvenci) TAGy (popisky/polepky), v jejichž čipu je natrvalo uloženo pouze unikátní číslo, a které jsou používány například pro zabezpečení zboží ve formě samolepícího štítku s čipem, nebo o složitější systémy, které obsahují čipy disponující omezenou výpočetní kapacitou pro zajištění výpočtů šifrovacího algoritmu. Čipy těchto karet umožňují zápis dat do definovaných datových sektorů (aplikací). Každý takový sektor může být zabezpečen čtecím a zápisovým klíčem, stejně tak je zabezpečena celá karta. Tyto typy karet jsou pak používány pro zabezpečené uložení malých objemů dat a jsou s výhodou používány v kartových systémech v rámci odbavení cestujících[5].

[4] Čárkovaná oblast není předmětem tohoto příspěvku
[5] Technické specifikace jsou uvedeny v normě ISO 14443

Zvláštními typy bezkontaktních čipových karet jsou karty duální a hybridní. Duální kartou je možno nazvat nosič, který obsahuje dva a více autonomních systémů, přičemž se může jednat o systém kontaktní + bezkontaktní, bezkontaktní + bezkontaktní, kdy každý systém pracuje na jiném kmitočtu a je používán pro jiné aplikace. Kombinace bezkontaktní a kontaktní technologie je používána například v produktu Visa paywave. Hybridní karta nabízí pro kontaktní čip bezkontaktní rozhraní.

Duální a hybridní karty jsou doménou bankovního prostředí, avšak začínají se stále ve větší míře prosazovat na dopravním trhu – jejich bezkontaktní část je možno, za splnění určitých podmínek, použít v odbavovacích systémech, jedná zejména o hrazení mikroplateb bankovní elektronickou peněženkou – elektronickými penězi[6]. Praktickým příkladem může být Bratislavská Mestská karta[7].

Technologie NFC

NFC - Near Field Communication – technologie bezdrátové komunikace o vysokém kmitočtu na krátkou vzdálenost. NFC je pouze technologií komunikačního rozhraní, nejedná se tedy o bezkontaktní kartu v mobilním telefonu. Technické parametry rozhraní jsou následující:

- NFC je bezkontaktní technologie (cca 10 cm), 13,56 MHz,
- technologie je standardizována dle ISO 18092, ECMA[8] a ETSI[9],
- technologie je kompatibilní s ISO 14443 (Mifare).

Mobilní telefon vybavený rozhraním/technologií NFC a dalšími nezbytnými prvky, které jsou uvedeny níže, umožňuje:

- zabezpečenou komunikaci, šifrování dat,
- zabezpečenou dálkovou správu aplikací na zabezpečeném servisním kanálu operátora,
- stávající infrastruktura odbavovacího systému zůstává beze změn (není třeba výměna čteček bezkontaktních karet).

Technologie NFC umožňuje výměnu dat – komunikaci ve třech módech:

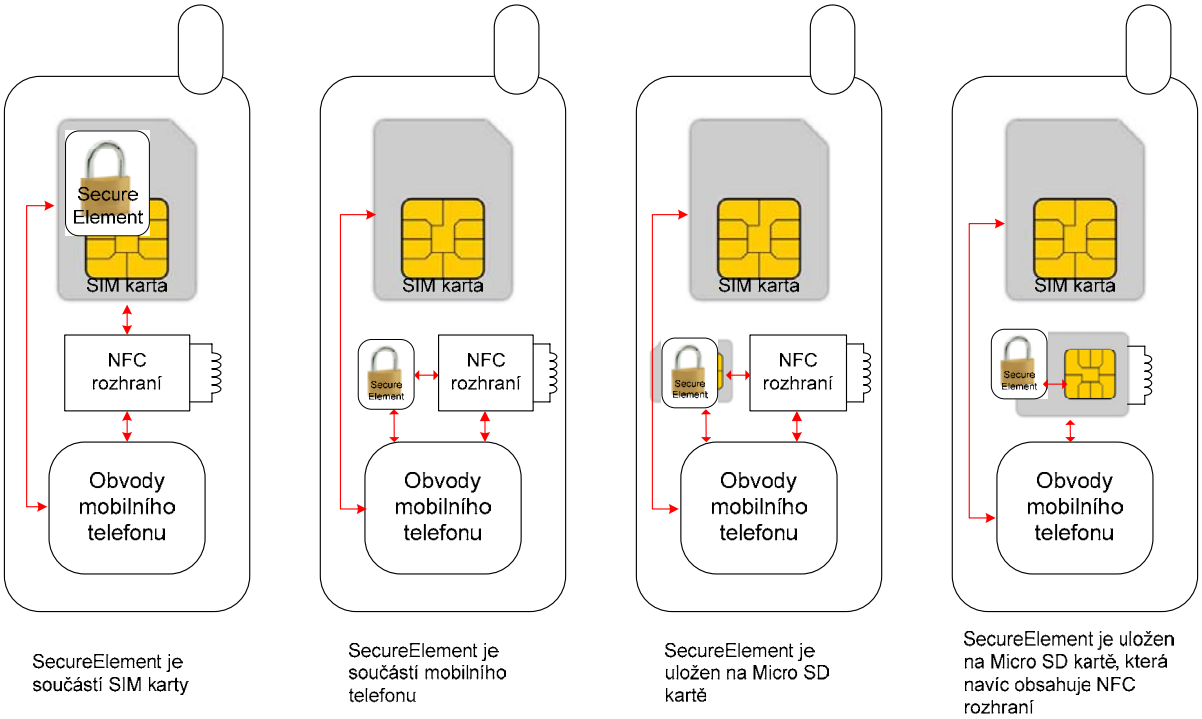
- Peer to peer (jeden s druhým):
  - komunikace mezi rovnocennými zařízeními (podobně jako BlueTooth) dle ISO18092,
  - obě NFC zařízení jsou aktivní.
- Reader/Writer (čtení/zápis) mód:
  - NFC zařízení funguje jako NFC čtečka,
  - NFC zařízení je aktivní.
- Emulace čipové karty:
  - NFC zařízení je pasivní,
  - využívá čteček bezkontaktních čipových karet.

[6] Pojem elektronických peněz a jejich vydávání upravuje Zákon č. 139/2011 Sb., kterým se mění zákon o platebním styku a některé další zákony
[7] http://www.karta.bratislava.sk/
[8] European Computer Manufacturers Association (ECMA)
[9] European Telecommunications Standards Institute (ETSI)

Obrázek 2 - Módy komunikace mobilního telefonu s NFC rozhraním

Využití mobilního telefonu s rozhraním NFC jako nosiče bezkontaktní čipové karty - přesněni řečeno jako nosiče její struktury aplikací a příslušných zásad zabezpečení – příslušných klíčů, je podmíněno:

- emulací bezkontaktních čipových karet na SIM kartě/microSD kartě, v mobilním telefonu,
- **zabezpečeným uložením** dat v SecureElementu na SIM kartě/microSD kartě, v mobilním telefonu,
- **implementací TSM** (Trusted Service Manager – služba pro komunikaci s bezpečným prvkem v mobilním telefonu, v tomto případě Secure Element na SIM) a **OTA** (Over The Air – systém pro distribuci nových versí SW a konfiguračních parametrů do mobilního telefonu)**,**
- zajištěním **bezpečné komunikace TSM** se **SIM.**



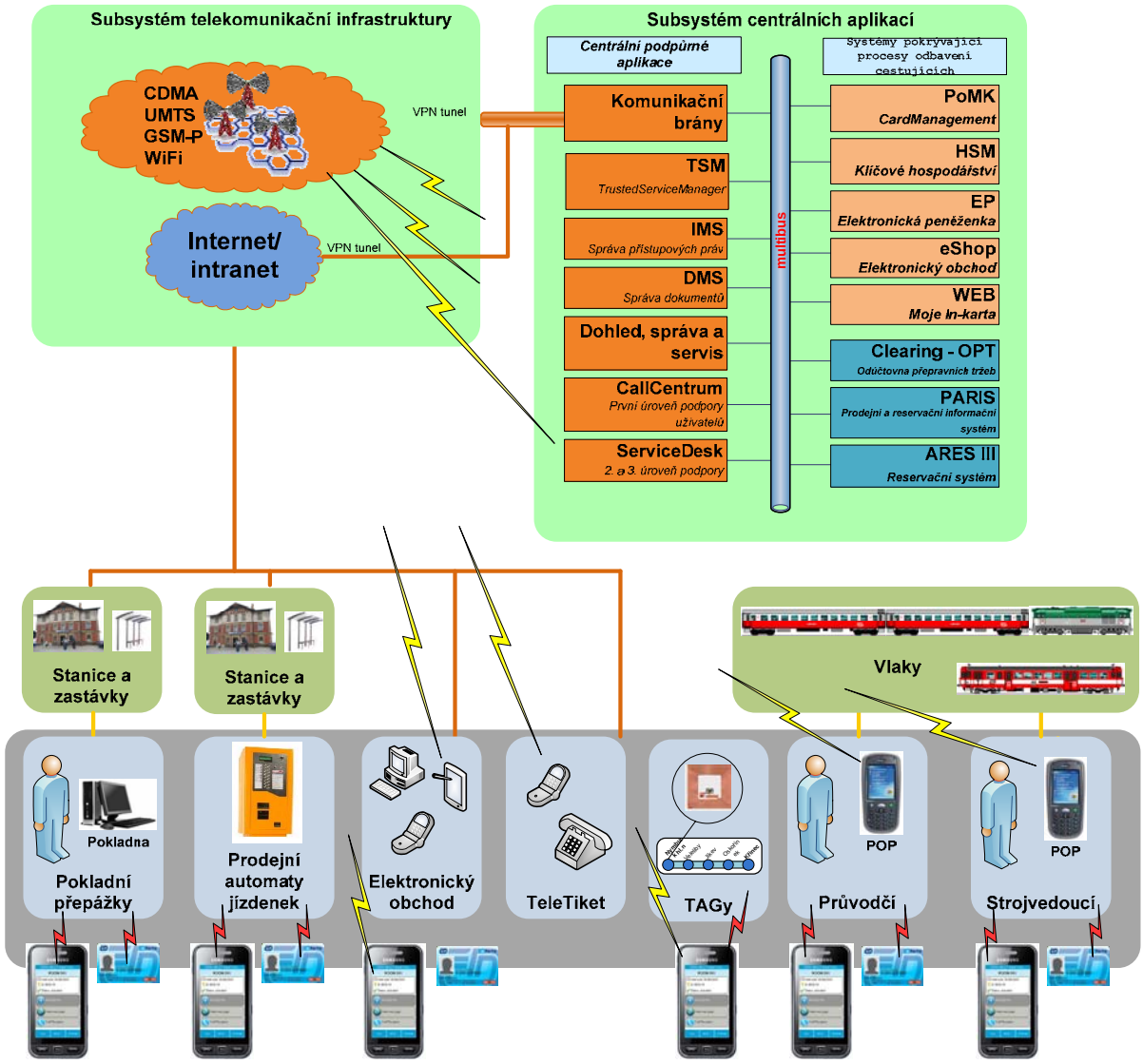
Obrázek 3 - Možnosti umístění SecureElementu v mobilním telefonu [4]

Obrázek 3 představuje možnosti umístění SecureElementu v zařízení mobilního telefonu. Funkci SecureElementu je možno si představit jako funkci čipu v bezkontaktní čipové kartě. V SecureElementu jsou podobným způsobem uloženy aplikace a jejich datový obsah v souladu s pravidly uvedenými výše v požadavcích na technický nosič dat. Ke čtení a zápisu datového obsahu do aplikací je tedy třeba, stejně jako v případě čipových bezkontaktních karet, klíčů.

Varianty umístění SecureElementu vycházejí z možností výrobců mobilních telefonů a z možností operátorů mobilních sítí. Každá varianta s sebou nese určité výhody a nevýhody. Z hlediska operátora je patrně nejvýhodnější umístění SecureElementu na SIM kartě, která je v jeho vlastnictví. Vydavateli bezkontaktní čipové karty (zpravidla IDS, dopravci, municipality) přináší však nutnost ukládat aplikace a jejich datový obsah na SIM kartu, kterou fysicky nevlastní ani nespravuje. Tato situace je však řešitelná volbou vhodného obchodního modelu a vhodného technického řešení správy aplikací.

Personalizace karty v SIM je na straně mobilního operátora pokryta systémy TSM[10] a OTA. Při požadavku zákazníka na personalizaci karty zasílá CardManagement informaci do TSM, který připraví data pro provedení personalizace karty v SIM. Data jsou po té odeslána prostřednictvím systému OTA servisním kanálem operátora. Informace o úspěšně provedené personalizaci je zpětně zaslána do systému CardManagenentu.

[10] Není podmínkou, aby byl využíván TSM mobilního operátora (tzv. single mód), existuje varianta delegated mód, kde je systémem TSM vybaven také karetní operátor, TSM pak slouží jako rozhraní k ostatním mobilním operátorům



Obrázek 4 .- Odbavovací systém s bezkontaktní technologií, příklad odbavovacího systému ČD - výhled

Obrázek 4 představuje možnou architekturu řešení zapojení mobilní technologie do odbavovacího systému, ve kterém jsou využívány bezkontaktní čipové karty. Mobilní operátor provádí na základě požadavků vydavatele karet správu aplikací v mobilním telefonu a umožňuje jeho držiteli využívání uložených aplikací.

Systém zabezpečeného uložení struktury aplikací bezkontaktní čipové karty do SIM mobilního telefonu umožňuje nezávislé ukládání struktur karet různých vydavatelů, což současná používaná technologie bezkontaktních čipových karet na standardu Mifare DESfire ev1 8kB umožňuje pouze omezeně a přináší s sebou řadu úskalí v oblasti procesů životního cyklu karty a CardManagementu.

Mobilní telefon musí být vybaven aplikačním SW, který umožní komunikaci uživatele s kartami uloženými na SIM. Aplikace na mobilním telefonu pak umožní držiteli pohodlné přepínání mezi jednotlivými „kartami“ například integrovaných dopravních systémů.

Jako problematický se do budoucna jeví větší počet typů mobilních telefonů, které s sebou nese větší rozmanitost jak HW, tak SW a zejména druhů operačního systému. Pro telefon vybavený rozhraním NFC, který umožňuje ukládání karet do SIM, bude nutno upravit aplikaci – rozhraní – uživatel vs. uložené karty a zřejmě ne každý takový telefon bude podporován.

Závěr

Na místě závěru je nutno říci, že odbavovací systémy, alespoň prozatím, nestojí ani nepadají na použití bezkontaktních technologií (srovnání: odbavovací systém IDS JMK – prozatím nemá vlastní karetní systém – připravuje se, vs. PID – karty jsou nosičem předplatních kupónů, přičemž oba systémy jsou plně funkční).

Je bezesporu, že bezkontaktní technologie je přínosem pro další rozvoj odbavovacích systémů, a to jak v oblasti způsobů odbavení, tak v oblasti rozúčtování, dopravních průzkumů a zvýšení komfortu cestujících/zákazníků.

Přechodem bezkontaktní karty do mobilního telefonu se dostává bezkontaktnímu odbavení nové dimense.

Bezkontaktní karta převedená do mobilního telefonu umožňuje on-line komunikaci s centrální částí odbavovacího systému, její držitel může prostřednictvím SW v mobilním telefonu s kartou interaktivně pracovat – vidí na displeji mobilního telefonu aktuální stav aplikací, vidí zůstatek stavu elektronické peněženky, dokonce může volit IDS, ve kterém se pohybuje. Karta je vydávána a spravována vydavatelem na dálku – držitel nečeká na její výrobu a personalizaci. Z „obyčejného“ odbavovacího systému se stává dopravně-telematický systém.

Literatura

[1] Nařízení vlády č. 295/2010 Sb., ze dne 20. října 2010 o stanovení požadavků a postupů pro zajištění propojitelnosti elektronických systémů plateb a odbavení cestujících a dále Příloha č. 1.

[2] Nařízení vlády č. 295/2010 Sb., ze dne 20. října 2010 o stanovení požadavků a postupů pro zajištění propojitelnosti elektronických systémů plateb a odbavení cestujících a dále Příloha č. 2.

[3] Zákon 194/2010 Sb. - Zákon o veřejných službách v přepravě cestujících a o změně dalších zákonů

[4] Gajdos, M. - Kozler, M: Has our relationship with money and spending changed?, *CARDS 2011. Conference 18 – 19 October 2011, Praha*

Praha, říjen 2012

Lektoroval: Ing. Jan Šimůnek
ROPID