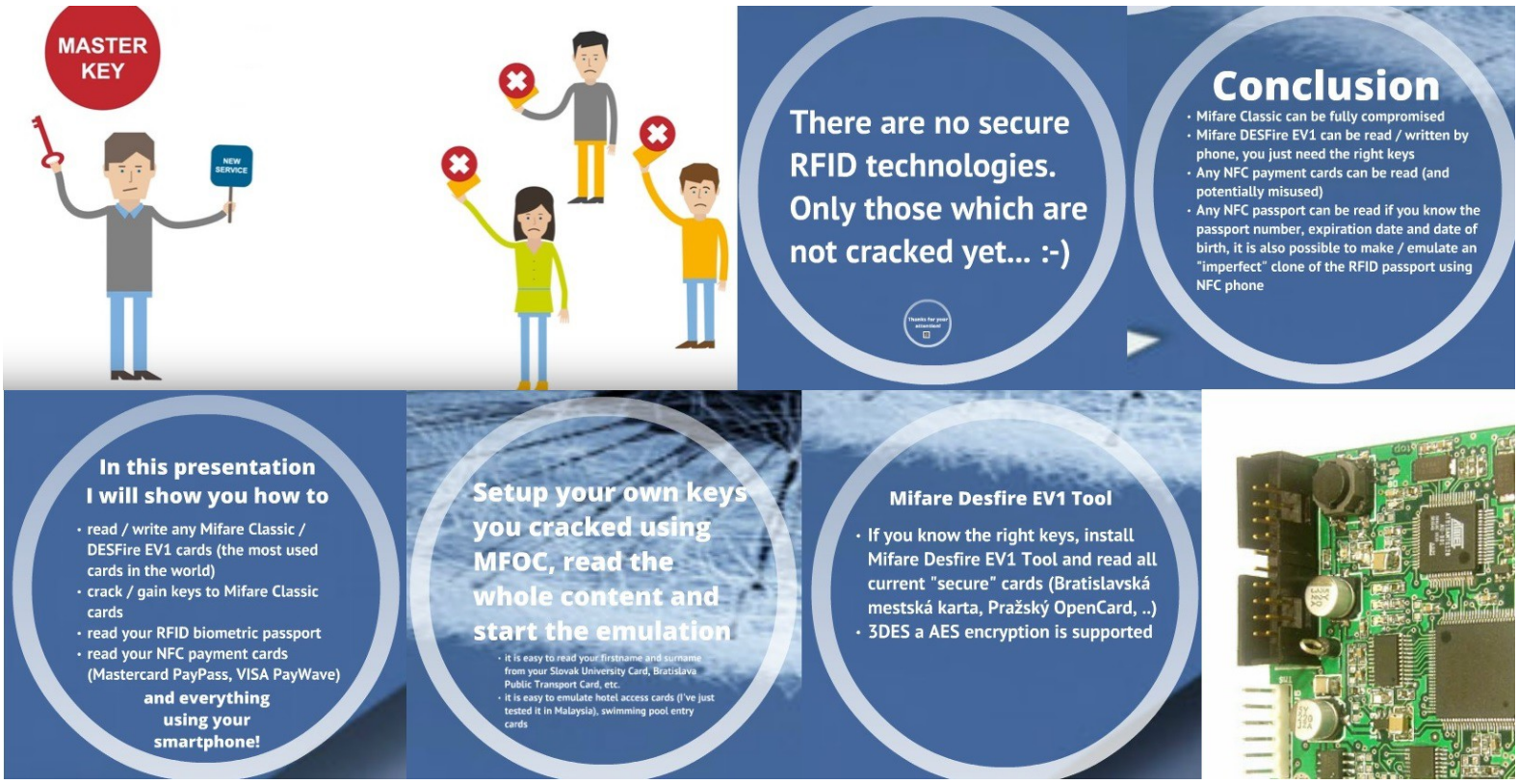

Ukázka nebezpečí RFID/NFC smart karet a souvisejících technologií, systémů. – Zdroje obrázků: Certifikovaný bezpečnostní IT expert a výkonný ředitel společnosti „NETHEMBA S.R.O.“ pan „PAVOL LUPTÁK“, https://prezi.com/akekjqnu0uqz/hacking-rfid-devices-using-nfc-smartphones-workshop/; NXP Semiconductors, https://youtu.be/v6tTQqAiVfU

Ostravský magistrát potvrdil závažná rizika dálkově čitelné tzv. „jízdní karty“ ODISky! IT odborníci Unucka a Lupták důrazně varují před bezmyšlenkovitým podceňováním nebezpečí těchto karet! Tzv. „motivační vnucování“ ODISek spotřebitelům, kteří je neumějí nebo nebudou plně využívat a ani si neuvědomují problémy, které jim mohou kyberzločinci díky tzv. „smart kartám“ způsobit, představuje nehorázný hazard se životy nevinných občanů! – Vážený ostravský občan/senior Petr Hadaščok nst. (podrobnosti k jeho činnosti a názorům viz. např. zde) a Vážený pan Mgr. Radek Přepiora (publicista, šéfeditor webu Společenství Necipujtenas.CZ) vystoupili v minulých měsících (2016 a 2015) v rámci veřejné diskuse na Zastupitelstvu Statutárního města Ostravy se svými podněty a dotazy k reálným nebezpečím tzv. ostravské „chytré karty“ ODISka. Zaměstnanci ostravského Magistrátu (MO) si posléze sami pečlivě pročetli zápisy z jednání zastupitelstva a pokusili se výše uvedeným občanům zprostředkovat odpovědi ve spolupráci se společností Koordinátor ODIS s.r.o. Z písemného stanoviska MO ze dne 14. března 2016 následně vyplynuly mj. následující závažné skutečnosti: Předně byly potvrzeny oprávněné obavy občanů ve věci kybernetické nebezpečnosti ODISky, která má podle vyjádření MO „*potřebná data nahrána přímo na ní*“. – Díky tomu samozřejmě existuje dle již dříve zveřejněných informací Společenstvím webu Necipujtenas.CZ (viz níže ve zdrojích) nebetyčné riziko klonování každé takové karty a zjištění/použití tzv. „master klíče“, pomocí něhož lze měnit za využití čteček jakákoliv data ať již na samotných nosičích ODISek nebo v patřičných systémech apod. Vždyť už i běžní uživatelé Internetu vědí: cokoliv jednou umístíte do digitálního prostředí, tak je to zkrátka odtajněno; nějaké ujišťování o zabezpečování takových dat nebo jejich mazání je naprosto irelevantní. K citlivým informacím se lze dostat v určité podobě i po jejich destrukci. Co jednou digitální prostředí a Internet schvátí, to se již do soukromí a utajení nikdy zpátky nenavrátí. Vždyť stačí i jen sekunda k tomu, aby došlo k získání/zneužití dat a související informace. I za tak krátkou dobu mohou citlivé údaje obletět takřka celý svět a dostat se na milióny různých nosičů. – Dopis MO v této věci uvádí, že zpracovatel osobních dat, která musejí uživatelé ODISek poskytnout, s nimi nakládá pouze na samém začátku procesu výroby karet a to po dobu maximálně tří měsíců; společnost Koordinátor ODIS s.r.o. k tomu ovšem připojila vágní ujištění o naprosté bezpečnosti celého procesu zpracování a nakládání s osobními údaji. – Jenže paradoxně opět výše uvedené stanovisko MO ze dne 14. března 2016 jednoznačně připustilo následující bezpečnostní problém ODISek: „*Tzn., že i kdyby došlo k prolomení bezpečnosti karty a někdo dokázal vyčíst, co na kartě je, tak jedinou informací, kterou je schopen se dovědět je, že na kartě je uložen např. profil opravňující k nákupu nějakého slevového kupónu nebo je na kartě zapsaná jízdenka.*“ A dále text přípisu MO v tomto případě přiznává, že kyberzločinec by mohl třeba kartu neoprávněně „*využít na jízdy*“ v městské hromadné dopravě na úkor právoplatného držitele ODISky. Za technické zabezpečení ODISky zodpovídá samotný Koordinátor KODIS s.r.o. – Ovšem karta ODISka samozřejmě obsahuje navíc také funkci tzv. elektronické peněženky, se kterou se dá rozsáhle pracovat, získávat z ní neoprávněně a dokonce na značné vzdálenosti bez vědomí vlastníka finanční prostředky včetně osobních identifikátorů nebo monitorovat zvyky konkrétní osoby. Elektronickou peněženkou v ODISce lze bezkontaktně platit v omezeném množství a částkách také ve vybraných

obchodech, terminálech, Internetu apod., které podporují technologie RFID/NFC rychlých plateb. Na kartě ODISka je sice fotografie jejího majitele, nicméně na tu se nikdo z obsluhy třeba v obchodě při použití rychlých/bezkontaktních plateb elektronické peněženky nedívá ani ji nekontroluje. Sofistikované technologické systémy, které párují fotografii na kartě s kamerovým rozpoznávání tváří nakupujícího se zatím ještě ve velké míře v ČR nepoužívají. – Dopis MO dále vysvětluje, že v případě zneužití ODISky dojde k „*zablokování použití karty*“, které „*se pohybuje do 24 hodin*“. „*Nejdéle se uvádí 3 dny.*“ – Jenže tohle je naprosto neskutečně dlouhá doba. Žijeme přeci ve světě, kde lze uskutečňovat digitální operace/elektronické transakce i během jedné vteřiny. Poškozená osoba se dozví o své finanční ztrátě mnohdy až za několik týdnů ze svého výpisu karetních transakcí. Navíc nynější legálně stanovené malé limity na kartách pro bezkontaktní placení nejsou věčné. – Na nebezpečí RFID/NFC karet typu ODISka s čipem „MIFARE DESFire EV1 8 kB“ (viz technická specifikace a možnosti využití ODISek popsané v článku zveřejněném přímo na stránkách Moravskoslezského kraje) již dlouhodobě upozorňuje ve svých přednáškách Vážený pan Pavol Lupták (certifikovaný bezpečnostní IT expert a výkonný ředitel slovenské IT společnosti Nethemba s.r.o.). Společenství webu Necipujtenas.CZ o něm psalo mj. v březnu 2015. Jeho stále aktuální prezentace připravená na základě rozsáhlých testů mnoha RFID/NFC nosičů dat ukázala zcela natvrdo: jak nebezpečné dokáží být „chytré karty“ pro své uživatele již jen za pomoci běžně dostupných aplikací pro chytré mobilní telefony. Lze s nimi posléze např. třeba takovou ODISku nejen číst, získávat karetní bezpečnostní klíče, nýbrž také přepisovat nebo klonovat informace na nové („prázdné“) karty, které jsou posléze při opatrném stylu používání automatickými systémy jen těžko detekovatelné. Pan Lupták velice správně vysvětlil: Neexistuje bezpečná RFID/NFC technologie. – Navíc pro ty lidi, kteří s chytrými technologiemi neumějí zacházet, neuvědomují si jejich rizika, ale přesto jsou k jejich používání tzv. „motivačně nuceni“ bez možnosti jiné a férové metody prokazování jízdného (senioři), jde o vysloveně nebezpečný hazard. Velice tristní je pak to, pokud se na něčem takovém navíc podílejí někteří politici. – Ostatně stačí např. vzpomenout dramatické selhání chytrých jízdních karet, které mohla překvapená veřejnost sledovat na počátku roku 2016 v Londýně. – K nebezpečím ODISek a mj. k souvisejícím rizikům datových systémů se pro Necipujtenas.CZ vyjádřil v dubnu 2016 například také Vážený pan Ing. Jakub Unucka, MBA, jeden z nejuznávanějších expertů na otázky RFID/NFC technologií v ČR, lídr ODS pro letošní krajské volby v MS kraji a místostarosta Klimkovic: „*K těmto datům má přístup prakticky kdokoliv: pokladní, vedení prodejny, majitel prodejny, správce software, správce hardware, operátor, banka…… Riziko tedy není samotný akt nákupu, ale datová stopa, kterou platba zachová. Pokud se jí obávám, mohu platit hotově. Stejné je to při platbě v autobusu nebo tramvaji. Pokud platím kartou, ať už ODIS nebo platební, opět vzniká o mé cestě lehce zneužitelná elektronická stopa. Nejen o nástupu, ale i výstupu. Pokud se jí bojím, mám mít možnost tuto stopu nezanechat. Pracujeme s různými softwarovými systémy a vím, že k datům má na pozadí přístup mnoho osob, bez ohledu na zabezpečení. Proč háčkovat nějaký software, když můžu navštívit kamaráda, který s daty pracuje……. Opět platí, že občan by měl mít právo použít takovou metodu, která nezanechá elektronickou stopu.“ – „Každý občan má mít právo provést úkon tak, aby o něm nezůstala elektronická stopa, vztahující se k dobrovolným a neúředním úkonům. Nemám problém s přečtením čipu v občanském průkazu při návštěvě budovy soudu. Ale mám problém se sejmutím čísla ODIS karty, pokud se vracím domů ze Stodolní v pět ráno.*“ – Elektronická odpověď MO z 21. 3. 2016 na doplňující dotaz Váženého Petra Hadaščoka nst. ke všemu přinesla následující velice zajímavé skutečnosti, které otevírají nové otázky obzvláště se vztahem k výběru výherce veřejné zakázky tzv. „systému zpracování dat“ ODISek: „*Dobrý den pan Hadaščoku, s Vašimi dalšími dotazy ke kartám ODISka jsem se obrátil na odborníky, kteří zajišťovali veškeré procesy vedoucí k zavedení těchto karet do provozu. Tito se vyjádřili k Vašim dotazů takto: E-karty ODISka byly součástí výběrového řízení pod názvem „Zákaznický portál“, které bylo vypsáno 11. 05. 2010 formou zakázky malého rozsahu. Byly osloveny čtyři firmy a Dopravní podnik Ostrava a.s. zároveň zveřejnil výběrové řízení na veřejně dostupném portálu elektronického systému ppeSystém. Nabídku podal pouze jeden uchazeč, a to společnost TELMAX s.r.o. Dopravní podnik Ostrava a.s. nastavil hodnotící kritéria podle ekonomické výhodnosti. Jednotlivá dílčí hodnotící kritéria byla: technické řešení s 60% váhou a kritérium ceny s váhou 40%. Zákaznický portál v současnosti provozuje Koordinátor s.r.o. a slouží všem dopravcům v ODIS. Cena ODISky je stanovena jednotně v rámci integrovaného dopravního systému ODIS, tedy všichni dopravci jsou vázáni ji uplatňovat ve stejné výši. Cena odráží náklady na vyhotovení karty včetně její personifikace a její distribuci cestujícímu.*“ – Řešení celé situace s ODISkami, kolem kterých se navíc objevují také závažné etické otázky v souvislosti s našimi i zahraničními věřícími (např. pravoslavnými, židovskými, ortodoxními ale také mnohými dalšími) spoluobčany, přitom spočívá v diverzifikaci rizik. Nelze protěžovat pouze jednu jedinou metodu prokazování jízdného. Společenství webu Necipujtenas.CZ (SwN) takové řešení již předložilo vedení ostravské radnice. Na 5. května 2016 je v této záležitosti připraveno pracovní jednání s patřičnými osobami, které o ODISkách v Ostravě oficiálně rozhodují. – SwN tímto děkuje Váženému panu Hadaščokovi nst. a pověřeným zaměstnancům ostravského Magistrátu za zprostředkování a zaslání důležitých informací. Díky tomu jsme mohli informovat širokou veřejnost. – SwN nijak nepodporuje nucení kohokoliv k povinnému přijetí mikročipů nebo jakýchkoliv moderních technologií např. formou legislativního aj. násilí nebo prostřednictvím tzv. „motivačního vymáhání“. Každému musí být umožněn svobodný opt-out, aby nemusel mikročipy nebo jiný typ svého označení povinně akceptovat a nebyl také díky takovému svému rozhodnutí diskriminován. Opačný přístup slouží Zlu! Důrazně se v této souvislosti distancujeme od jakéhokoliv schvalování forem legislativního násilí a neférových praktik nesvobodné hospodářské soutěže, které např. protěžují pouze technologii externího nebo interního

čipování na úkor jiných, přitom daleko lepších, úspěšnějších, svobodnějších, mnohdy levnějších a především neinvazivních řešení! Nikomu zároveň nelze bránit v dobrovolném sebeočipování, označení, se všemi známými riziky pro jeho tělo, peněženku i lidskou duši. – Dokumentace je k dispozici níže.

Zdroj: Elektronická a telefonická komunikace s Váženým ostravským občanem/seniorem Petrem Hadaščokem nst. (podrobnosti k jeho činnosti a názorům viz. např. zde) ze dnů 17. až 21. března 2016; dokumentace zaslaná Magistrátem Statutárního města Ostravy Váženému panu Hadaščokovi nst. a Váženému panu Mgr. R. Přepiorovi (publicista, šéfeditor Společenství webu Necipujtenas.CZ) pod číslem jednacím SMO/080414/16/OD/Foj s datem 14. března 2016; http://www.necipujtenas.cz/clanky-publikace-texty/unucka-proti-nedobrovolnemu-cipovani-cr.aspx; http://www.msk.cz/cz/bezkontaktni-cipova-karta-odiska-38061/; https://prezi.com/akekjqnu0uqz/hacking-rfid-devices-using-nfc-smartphones-workshop/; http://www.necipujtenas.cz/Files/necipujtenas/srlabs-reuters-motherboardmailonline-rt-karsten-nohl-european-card-rfid-microchipping-system-in-danger-hackers-on-the-rise-germany-eu-2015.jpg; http://www.necipujtenas.cz/Files/necipujtenas/tv-markiza-bbc-pavol-luptak-nethemba-martin-emms-aad-van-moorsel-newcastle-university-great-dangers-of-rfid-nfc-microchips-in-banking-system-slovakia-great-britain-2015-2014.jpg; http://www.necipujtenas.cz/Files/necipujtenas/defcon23-bishop-fox-francis-brown-great-dangers-of-rfid-nfcmicrochipping-hacking-odiska-usa-cr-2015-page-001.jpg; http://www.necipujtenas.cz/Files/necipujtenas/nxpsemiconductors-dutch-xt-card-tomas-valler-abbas-cr-tanenbaum-odiska-ostrava-dangers-of-rfid-microchips-2015-2010.jpg; http://www.necipujtenas.cz/fakta/rizika-cipovani/prof-tanenbaum-vazna-rizika-mikrocipu-nl.aspx; http://www.necipujtenas.cz/Files/necipujtenas/official-statement-russian-orthodox-church-moscow-patriarchate-againstmicrochipping-2013.pdf; http://www.necipujtenas.cz/Files/necipujtenas/mhd-ostrava-varianty-jizdneho-a-bezcipove-identifikace-cestujicich-necipujtenas-cz-svobodni-a-soukromnici-2016.pdf; http://www.necipujtenas.cz/Files/FckGallery/official-words-church-anti-microchippingchildren-dissent-russia-2013.jpg; http://www.telegraph.co.uk/news/uknews/road-and-rail-transport/12077955/Londons-Oyster-card-system-crashes-giving-thousands-free-travel.html; http://www.bbc.com/news/uk-england-london-35213346; http://www.independent.co.uk/news/uk/home-news/free-travel-in-london-as-oyster-card-reader-glitchcoincides-with-first-day-of-higher-fares-a6793631.html; http://www.theguardian.com/money/2016/jan/02/oyster-cardglitch-means-free-travel-for-london-passengers; http://www.standard.co.uk/news/transport/oyster-card-users-enjoyfree-travel-across-london-as-massive-technical-glitch-hits-payment-system-a3146841.html; https://twitter.com/TfLTrafficNews/status/683187019745464321; http://metro.co.uk/2016/01/02/oyster-card-readers-arent-working-so-tubetravel-is-free-5596234/; http://economictimes.indiatimes.com/news/international/world-news/london-commuters-getfree-ride-due-to-technicalglitch/articleshow/50416945.cms; http://www.theboltonnews.co.uk/news/national/14178262.display/; http://www.standard.co.uk/news/transport/oyster-card-users-enjoy-free-travel-across-london-as-massive-technical-glitch-hits-paymentsystem-a3146841.html; http://www.computerweekly.com/feature/Oyster-Card-The-highs-and-lows-of-Oyster; http://www.mirror.co.uk/news/uk-news/oyster-card-crash-means-free-7104935; http://www.ic3.gov/media/2015/150910.aspx

Statutární město Ostrava
Magistrát

Vaše značka:
Ze dne:
Č. j.: SMO/O80414/16/OD/Foj
Sp. zn.:

Vážený pan
Petr Hadaščok

Vyřizuje: Ing. Martin Fojtík
Telefon: +420 599 443 306
Fax: +420 599 442 034
E-mail: mfojtik@ostrava.cz

Datum: 2016-03-14

Vážený pane Hadaščoku,

odboru dopravy Magistrátu města Ostravy byl postoupen Váš dotaz, vznesený na zasedání zastupitelstva statutárního města Ostrava dne 17. 2. 2016 k problematice bezpečnosti bezkontaktní karty ODISka. Váš dotaz jsme předložili k vyjádření zástupci společnosti KODIS s.r.o., který nám k Vámi zmiňované problematice poskytl vyjádření.

Klasická bankovní, popř. věrnostní karta je kartou přístupovou, je zpravidla evidovaná na dané jméno a přístup je chráněn přes PIN k danému účtu, popř. jiným náležitostem. Karta ODISka však není identifikátor, není přístupová k žádnému účtu, potřebná data jsou nahrána přímo na ní. Po vydání karty ODISky držiteli se všechna osobní data, které spojují danou osobu s ODISkou vymažou a není možno je získat. Tento postup je právě nejvíce kritizován držiteli ODISek, jelikož každé prokázání držení ODISky ať už v případě reklamací, služeb, kontroly aj. musí prokazovat držitel osobním kontaktem na určeném místě, kde musí držitel karty prokázat, že karta je jeho. Je to ale daň za ochranu osobních údajů.

Důležité je, že na ODISce nejsou uložena žádná osobní data, jako např. RČ, adresa aj. Tzn., že i kdyby došlo k prolomení bezpečnosti karty a někdo dokázal vyčíst, co na kartě je, tak jedinou informaci, kterou je schopen se dovědět je, že na kartě je uložen např. profil opravňující k nákupu nějakého slevového kupónu nebo je na kartě uložena zapsaná jízdenka.

V případě, že jsou na kartě uloženy elektronické peníze, tato částka je velmi omezena výší a držitel ji může nechat okamžitě zablokovat, tzn. ten, kdo kartu odcizil, by ji mohl maximálně využít na jízdy. Ale jelikož je na kartě fotografie, obsluha může kartu zabavit, pokud ODISku drží někdo jiný než její držitel. Zablokování použití karty se pohybuje běžně do 24 hodin. Nejdéle se uvádí 3 dny. A dále, fyzicky peníze z karty může dostat vyplaceno opět pouze její držitel, po fyzickém kontaktu s obsluhou vydavatele, která peníze vyplatí pouze držiteli karty.

Při zavádění projektu byl hlavně kladen důraz na bezpečí osobních dat a také vyloučení možnosti jakéhokoli spojení dané karty s konkrétní osobou. Z tohoto důvodu bylo zakázáno uchovávat databáze držitelů. Vydavatelé mají za povinnost uchovávat data pouze na dobu nezbytně nutnou, a to dle povolení ÚOOÚ max. na dobu 3 měsíců, při kterých se tyto použijí max. pro reklamaci vyrobené karty z důvodu, aby nemusel držitel opětovně nosit fotografii apod.

Technické zabezpečení je momentálně jedno z nejmodernějších, nositelem bezpečnostní politiky ODISek je KODIS s.r.o..

K zaměstnaneckým kartám zaměstnanců krajského úřadu Moravskoslezského kraje (dále KÚ MSK) si Vám dovolujeme sdělit, že vydavatelem této karty je KÚ MSK a KODIS s.r.o. je pouze správcem dopravní aplikace na kartě. To jakým způsobem má KÚ MSK zaveden způsob bezpečnosti držitelů karet je věcí KÚ MSK, nicméně dopravní aplikace je naprosto shodná s kteroukoli jinou ODISkou, tzn. taktéž neobsahuje žádná osobní data a vše funguje naprosto stejně. Ani KODIS s.r.o., jako správce tohoto dopravního prostoru, nezná držitele daných karet a veškerou komunikaci a operace za držitele karet zajišťuje jejich zaměstnavatel.

Vážený pane Hadaščoku, věříme, že odpovědi na Vaše dotazy ohledně zajištění bezpečnosti bezkontaktních karet ODISka Vás přesvědčily, že nebylo ponecháno nic náhodě a karta ODISka splňuje veškeré náležitosti být bezpečnou součástí života cestujících prostředky veřejné linkové dopravy.

S pozdravem

STATUTÁRNÍ MĚSTO OSTRAVA
magistrát
- 20 -

Ing. Břetislav Glumbík
vedoucí odboru dopravy

Od: Fojtík Martin <MFojtik@ostrava.cz>
Komu: Petr Hadaščok <hadascokp@seznam.cz>
Datum: 21. 3. 2016 15:00:37
Předmět: ODISka

Dobrý den pan Hadaščoku,

s Vašimi dalšími dotazy ke kartám ODISka jsem se obrátil na odborníky, kteří veškeré zajišťovali veškeré procesy vedoucí k zavedení těchto karet do provozu. Tito se vyjádřili k Vašim dotazů takto:

E-karty ODISka byly součástí výběrového řízení pod názvem „Zákaznický portál", které bylo vypsáno 11.05.2010 formou zakázky malého rozsahu. Byly osloveny čtyři firmy a Dopravní podnik Ostrava a.s. zároveň zveřejnil výběrové řízení na veřejně dostupném portálu elektronického systému ppeSystém. Nabídku podal pouze jeden uchazeč, a to společnost TELMAX s.r.o.

Dopravní podnik Ostrava a.s. nastavil hodnotící kritéria podle ekonomické výhodnosti. Jednotlivá dílčí hodnotící kritéria byla: technické řešení s 60% váhou a kritérium ceny s váhou 40%.
Zákaznický portál v současnosti provozuje Koordinátor s.r.o. a slouží všem dopravcům v ODIS.
Cena ODISky je stanovena jednotně v rámci integrovaného dopravního systému ODIS, tedy všichni dopravci jsou vázáni ji uplatňovat ve stejné výši. Cena odráží náklady na vyhotovení karty včetně její personifikace a její distribuci cestujícímu.

Doufám, že jsme odpověděli na všechny Vaše dotazy, čímž se ale nebráníme v případě dalších dotazů podat další informace, samozřejmě bude-li to v našich silách.

S pozdravem a přáním pěkného dne

Ing. Martin Fojtík
vedoucí oddělení
silniční a drážní dopravy

Magistrát města Ostravy
odbor dopravy
Prokešovo náměstí 8, 729 30 Ostrava
T + 420 599 442 333
M + 420 603 234 180
E mfojtik@ostrava.cz
W www.ostrava.cz