„Technologické posouzení infrastruktury PCMS" pro zadavatele Magistrát hlavního města Prahy.

Svazek č.1

Sídlo společnosti:
VBC Vinohradská Business Centrum, Vinohradská 174, 130 00, Praha 3
tel.: +420 222 523 000
fax: +420 222 524 060
www.e-fractal.cz

Obsah dokumentu:

1. Identifikační údaje zhotovitele

Identifikační údaje zhotovitele

Jméno	Ing. Jiří Berger, MBA
Organizace	**e-FRACTAL, s.r.o.**
Adresa	Vinohradská 1597/174, Praha 3, 130 00
Telefon	+420 222 523 000
IČ	26428091
Fax	+420 222 524 060
E-mail	jiri.berger@e-fractal.cz

Statutární zástupce

Ing. Jiří Berger, MBA – výkonný ředitel a jednatel společnosti,
tel: 222 523 000,
Mobilní telefon: 603 434 861,
jiri.berger@e-fractal.cz

Kontaktní adresa

e-FRACTAL s.r.o., Vinohradská 1597/174, Praha 3, 130 00

Bankovní spojení

KB, Italská 2, Praha 2, č. účtu: 273559660257/0100

Odpovědný řešitel projektu

Ing. Jiří Berger, MBA

Kontaktní osoba

Josef Blažek
Josef.blazek@e-fractal.cz
Mobilní telefon: 602 459 795

2. Předmět plnění

Předmětem plnění je **„Technologické posouzení infrastruktury PCMS"** pro zadavatele Magistrát hlavního města Prahy (dále jen MHMP).

PCMS – Prague Card Management System

2.1. Služby soudního znalce

Služby analýzy ICT a technologické forenzní zkoumání jsou poskytovány v přímé návaznosti na služby soudního znalectví, které je vnitřní součástí společnosti e-FRACTAL. Touto specializací jsme doplnili portfolio nabízených služeb o velmi žádanou oblast expertních znalostní v oblasti výpočetní a mobilní techniky a bezpečnosti informačních systémů, doplněnou o statut soudního znalce v této oblasti.

Již od počátku poskytování služeb analýzy ICT a technologického forenzního zkoumání jsme se zaměřili na zpracování a tvorbu podrobných metodických postupů, které jsou základem každého řešeného postupu. V oblasti IT lze na mnoha místech výhodně využít výsledky forenzní počítačové vědy.

Uplatnění technologických forenzních metod lze hledat na místech, kde se provádí analýza jevů a procesů spojených zejména s bezpečnostními incidenty nebo návrhy a realizací technologických řešení v souladu se specifikací, tj. tam, kde se požaduje hodnověrné, nezávislé a prokazatelné zjištění toho, co se v ICT stalo, za jakých podmínek a zda to bylo v souladu se standardy, případně specifikací.

2.2. Postup - analýza

Práci na zpracovávaném dokumentu jsme rozdělili do několika fází:

V první fázi jsme pracovali s důkladnou analýzou požadavků, existujících procesů, původních zadání a specifikací a následným srovnáním s existujícím stavem ICT v úvodní fázi projektu, v níž jsme se zaměřili na identifikaci problematických, případně sporných oblastí, které jsme po konzultaci s MHMP následně rozpracovali do míry podrobnosti, která odpovídá cílům a určení výsledného dokumentu. Postupné iterační cykly rozpracovávaly další oblasti a definovaly různou úroveň detailu pro jednotlivé analyzované oblasti a procesy.

Ve druhé fázi jsme se zaměřili na soulad procesů s existujícími ICT systémy a v případě nejednoznačnosti nebo nesouladu jsme hledali a definovali společně s MHMP příčiny tohoto stavu do výsledného dokumentu, který obsahuje i následná opatření vedoucí k narovnání stavu.

Ve třetí fázi jsme se v analyzované ICT infrastruktuře zaměřili na bezpečnostní hlediska a to jak z procesního, tak z technologického hlediska.

V poslední, závěrečné fázi jsme se zaměřili na výstupy naší činnosti na možný budoucí rozvoj posuzovaného projektu, technologické aspekty, standardy a nové trendy a východiska v dané oblasti stejně jako na optimalizaci stávajícího řešení z pohledu potřeb zákazníků, trhu i uživatelů. Tato fáze probíhala paralelně v průběhu celého projektu.

Oblast plnění výsledného dokumentu je v následujících oblastech:

Zaměřili jsme se na posouzení technologické infrastruktury PCMS a to v počátečním a cílovém stavu z několika hledisek. Klíčovými oblastmi byla vhodnost vybraných technologií a vhodnost jejich kombinací včetně dodržení určených standardů z čehož plyne i související identifikace a stručný popis významných technologických, případně systémových chyb a nedostatků v dosavadní realizaci projektu PCMS. Posouzení se zaměřilo i na shrnutí licenční politiky, ochrany vlastnických práv a záručních podmínek souvisejících s projektem a infrastrukturou PCMS.

Součástí je i vyhodnocení bezpečnostních rizik a vymezení stěžejních rizik projektu a dalšího rozvoje. Ve všech těchto oblastech proběhl sběr informací a dokumentů. Vzhledem k mandátu, který nám byl dán zadáním projektu, jsme nehodnotili ekonomické a finanční parametry projektu, pokud nešlo o přímou souvislost s technologickým posouzením, jako je například změna technologie apod.

2.3. Metody a funkce

Jakékoliv analýzy podřizujeme přísným metodikám a postupům, které odvozujeme od technologických forenzních analýz, které tvoří významnou části námi poskytovaných služeb. Díky přístupu k nejnovějším technologiím udržujeme naše **znalosti neustále na** nejvyšší dosažitelné úrovni a sledujeme současné i budoucí trendy vývoje ICT, které okamžitě aplikujeme do oblasti našich analýz.

2.4. Harmonogram plnění

Harmonogram plnění:

Projekt „Technologické posouzení infrastruktury PCMS" byl rozdělen do těchto fází:

První fáze:

Předložení rozpracovaného dokumentu, pracovní verze, k posouzení zda dokument postihuje všechny oblasti, které od výstupu MHMP očekává, získání dalších podnětů, koordinace při získávání dalších informací, které se nepodařilo získat pro první fázi, možná oponentura ze strany MHMP. Předloženo 15.12.2009.

Druhá fáze:

Zapracování podnětů / vstupů z první fáze, rozpracování jednotlivých témat do podrobné analýzy, kompletace informací z informačních zdrojů.

Třetí fáze:

Předložení „Technologického posouzení PCMS", včetně znaleckého posudku na použité karetní technologie, který vypracoval soudní znalec v oboru kybernetika, odvětví výpočetní technika, specializace výpočetní a komunikační technika, bezpečnost informačních systémů. Odevzdání projektu k 10.1.2010.

2.5. Manažerské shrnutí

Historie projektu je datována do roku 2006, kdy byl na základě studie z roku 2005 vytvořen projektový záměr. Následný úspěšný pilotní projekt, který byl akceptován, vytvořil prostor pro projekt podpořený podnikatelským plánem spustit elektronickou peněženku, která by zajistila příjmy z jednotlivých transakcí třetích stran a současně zajistila identifikační a platební nástroj pro obyvatele a návštěvníky HMP.

Původním předpokladem byl záměr vytvořit široce přijímanou platformu pro mikroplatby, což však přinášelo riziko v nutnosti disponovat v rámci projektu **bankovní licencí**, která je pro podobné mikroplatební systémy potřebná a to počínaje 1. lednem 2003. Toto ustanovení lze legislativně ošetřit formou výjimky, což i některé z karetních systémů v ČR využívají, ale vzhledem k množství vydaných karet je i při minimální částce, kterou by uživatelé na své kartě mohli mít, překročen finanční limit, v rámci něhož lze výjimku využít.

V době zpracování projektového záměru tedy bylo podceněno riziko neexistujícího reálného partnerství s bankovní institucí. Uživatelská základna, kterou je PCMS schopná vytvořit je však natolik zajímavá, že lze předpokládat **dobrou výchozí pozici pro jednání** s vybraným okruhem bankovních institucí, které by se mohly stát strategickým partnerem projektu. Z tohoto pohledu se jeví strategie zajištění klíčového počtu uživatelů díky zapojení aplikace elektronických předplatních kuponů MHD jako vhodný krok.

Technologicky a technicky je elektronická peněženka a s ní související aplikace a úpravy systému dle dostupných informací připravena, vzhledem k organizačně legislativním důvodům však zatím neproběhl pilotní a ověřovací provoz a karty neobsahují nahranou aplikaci pro elektronickou peněženku. Systém, který by měl obsluhu elektronické peněženky zajišťovat je od 30.6.2008 odstaven a neprobíhají v něm žádné transakce.

V rámci dalšího zkoumání jsme se zaměřili na ověření připravenosti testovacích scénářů a simulací pro ověření funkčnosti všech možností elektronické peněženky a připravenosti infrastruktury. V tuto chvíli je podobný **princip používán pro platbu parkovného**, ale vzhledem k výše uvedeným legislativně organizačním důvodům jej nelze plně zobecnit. Pro potřeby elektronické peněženky je nutné spustit zúčtovací centrum v plném režimu. Zúčtovací centrum běží v tuto chvíli z pohledu elektronické peněženky v částečném režimu, jelikož sice eviduje veškeré informace o parkovacích transakcích a je schopno v reálném čase zjistit zůstatek jakékoliv karty, ale neprobíhá v něm zúčtování jako takové, jelikož peníze nejsou vedeny na dedikovaném účtu, nad kterým by docházelo k zúčtovacím transakcím.

Dalším důležitým aspektem je podcenění rizika technologických nákladů souvisejících s akceptací karet. Vzhledem k tomu, že čtečky nelze poskytovat zdarma, nebo za symbolickou cenu, jelikož by šlo v případě

komerční sféry o veřejnou podporu a současně však nebyl nastaven efektivní mechanismus, který by motivoval komerční subjekty k investici do čtečky, která by elektronickou peněženku akceptovala, je nutné více **rozpracovat strategii založenou na tržních principech**.

Na základě probíhajících jednání lze konstatovat, že **komerční sféra má o podobná řešení zájem**, jelikož strategie řady bank je zavést mikroplatby (off-line platby) v případě transakcí do hodnoty cca 150 CZK. Bankám se sníží náklad na on-line autorizace/transakce a odpadne poplatek ve výši zhruba 3% za on-line transakce karetním asociacím (Visa/MasterCard). Motivace komerční sféry je v tomto případě v potencionální **cílovému kmenu 660 000** (aktuálně 385 000) držitelů Opencard, kdy komerční subjekty jsou ochotny investovat do akceptačních míst.

Technologické nedostatky

Systém byl na počátku spuštěn (rok 2006) s kartou MIFARE Classic i přesto, že v době spuštění již byla na trhu jiná, bezpečnější řešení včetně později použité MIFARE DESFire. Tento krok vycházel z předprojektové studie společnosti Soluziona, která byla následně v projektu naplněna. Konstatujeme, že existovalo i jiné možné řešení, které však nebylo v daném okamžiku realizováno. Přechod na bezpečnější karty MIFIRE DESFire probíhá v roce 2008 a jakmile vyprší dvouletá platnost původních karet MIFARE Classic (v průběhu února až května 2010), bude tento technologický nedostatek přirozenou obměnou karet odstraněn. Pro technologickou platformu PCMS to znamenalo dva různé způsoby komunikace karty s aplikací a také, vzhledem k tomu, že nová karta MIFARE DESFire obsahuje operační systém a šifrovací mikročip, zdvojení dalších vyvíjených prvků systému, jakými jsou oblast bezpečnosti, způsob ukládání dat na kartu apod.

Z předložených dokumentů jsme dospěli ke konstatování, že přestože je systém DOS provozován, vykazoval ke 30.6.2009 množství výhrad, které **DPP považuje za nevyřešené**. (Část z těchto výhrad byla vyřešena ve druhém pololetí 2009.)

Podpora a údržba systému je obvyklá dodávkám obdobného charakteru – rozsahem a danými parametry služby. Avšak díky špatně nastavené licenční politice (2006) je zde zřejmý značný nárůst ceny za službu jako takovou.

Identifikované procesní nedostatky

V průběhu zkoumání projektu byly nalezeny nedostatky v oblasti plánování a koordinace takto zadávaných služeb. Na projektu, od jeho samotného počátku, respektive v prvních měsících po zahájení projektu 2006, byla zvolena strategie **najímání externích odborníků třetích stran** do projektových týmů, které byly zodpovědné za projektové řízení.

Uváděným důvodem, pro tento postup, je nedostatečná kapacita odborníků s dostatečnou expertní znalostí a kompetencí v rámci MHMP. Tato strategie snížila možnou kontrolu projektu ze strany MHMP, současně však také došlo k opakované **změně subjektu**, který externí odborníky pro tuto oblast poskytoval a ze strany kompetentních osob MHMP byl tento stav pravděpodobně podceněn.

Při zkoumání byla získána projektová dokumentace odpovídající standardům vedení projektu zhruba od přelomu roku 2007/2008, podklady před touto dobou se nepodařilo získat v takovém rozsahu, aby bylo možné vyvodit závěry o způsobu vedení projektů a o projektovém řízení.

Komplex smluv na dodávky, licence, údržbu a na provoz je nutné řešit komplexní technologickou a smluvní strategií a teprve následně se zaměřit na jednotlivé části. Vzhledem k velmi diskutovaným smluvním vztahům a licenční politice je potřebné zacílit hlavní úsilí projektového řízení v rámci projektu Opencard na **získání komplexní kontroly nad projektem** a to ve všech jeho oblastech, tedy kromě projektové, organizační a technologické i nad souvisejícími oblastmi, tedy zvláště ekonomickou a právní. Dle zápisů z projektových schůzek a jednání jsme ověřili, že kroky k nápravě stavu do podoby podmínek, které by nastavily parametry projektu do podoby akceptovatelné pro MHMP, byly zahájeny na konci roku 2008, přesto se nepodařilo stav k 30.6.2009 jakkoliv upravit. Nad časový rámec daný zadáním tohoto dokumentu jsme získali informace, že v průběhu prosince 2009 byly dojednány některé klíčové změny pro další pokračování projektu. Vzhledem k tomu, že tato jednání stále probíhají a není z nich poskytován oficiální výstup, nepovažujeme za vhodné, jakékoliv detaily z této budoucí dohody uvádět do tohoto dokumentu.

V roce 2005 proběhlo předběžné oznámení projektu na centrální adrese. Následná **veřejná zakázka však byla v roce 2006 vyhlášena s výrazně vyšší cenou** (90 miliónů oproti původním 7 miliónům). V průběhu posuzování se nepodařilo získat podklady, které by tento nárůst objasnily.

Počáteční nastavení smluvních vztahů v projektu bylo z pohledu HMP nevýhodné a společnosti Haguess, jako komerční subjekt, tím získala a **využila veškerého vyjednávacího prostoru**, které mu smluvní ujednání z roku 2006 a předně způsob řízení projektu objednatelem dovolilo.

HMP v oblasti licencí zcela přistoupilo na nabízený licenční model, **aniž by proběhla odborná oponentura**, zda je pro HMP takový model akceptovatelný a výhodný. Pokud by v počáteční fázi projektu HMP lépe hájilo své zájmy, byly by pravděpodobně licenční podmínky nastaveny tak, aby nedocházelo ke zbytečnému, duplicitnímu, nebo neefektivnímu započítávání licencí karet, které aktivně systém nevyužívají nebo nebudou využívat.

Při posuzování licenční politiky jsme dospěli k názoru, že dle smluvní úpravy platné ke 30.6.2009, tedy k datu ke kterému je zpracováváno toto posouzení, je licence počítána **za každou kartu evidovanou v systému**, včetně karet, které byly z jakéhokoliv důvodu zrušeny, případně expiruvala jejich platnost (původní karty MIFARE Classic mají platnost 2 roky, stávající MIFARE DESFire mají platnost 4 roky). Z tohoto principu plyne teoretický výpočet, že po 4 letech, kdy uplyne platnost stávajících karet, bude nutné zdvojnásobit počet licencí, jelikož v systému budou kromě aktivních karet pro každého uživatele uloženy i informace o jeho předchozí kartě, případně o předchozích kartách! MHP doporučujeme změnit v rámci jednání se společností Haguess smluvní podmínky tak, aby byly licenční poplatky účtovány pouze za aktivní karty, využívající alespoň jednu z poskytovaných aplikací. Stávající karty MIFARE DESFire mají ve své datové položce uloženou identifikaci karty, která byla předchůdcem karty vydané, ale způsob evidence lze realizovat i ve formě smluvních reportů a pravidelných vyúčtování.

V souvislosti s výše uvedenými informacemi jsme zjistili, že pouze 260 tisíc z celkových 385 tisíc karet má nahraný některý z předplatných kupónů MHD, z čehož plyne, že určité část karet **byla uživateli pouze vyzvednuta bez toho, že by byly používány.** Důsledkem tohoto stavu je část vynaložených nákladů na vydané karty a současně významná část licenčních poplatků je vynakládána aniž by dané Opencard využívaly jakoukoliv aplikaci a byly zapojeny do systému. Jedním z efektivních modelů by mohla být platba jen za ty karty, které by systém opakovaně využily.

Projektové řízení v období změny karetní technologie bylo pod vedením společnosti Soluziona (dnes Indra). Doporučení původní technologie MIFIRE Classic pro pilotní provoz a jeho následné nahrazení technologií MIFIRE DESFire je v souladu s původní předprojektovou studií společnosti Soluziona „Pražské centrum kartových služeb" datovanou do roku 2005. Z tohoto pohledu konstatujeme, že problém změny karetní technologie **přisuzujeme špatnému projektovému rozhodnutí v době realizace projektu (2006, 2007)**, kdy se podmínky nasazování jednotlivých typů karet od původní studie změnily. Volba karty MIFIRE Classic pro pilotní projekt, namísto v době již běžně využívané karty MIFARE DESFire pak v konečném důsledku znamenala zbytečně vynaložené náklady na pořízení více jak 45 050 karet, které nebyly nikdy využity, a současně vedla k placeným úpravám celého systému. Rozdíl ceny obou karet v daném čase není při zvoleném počtu karet dostatečně významný, aby vynaložené náklady na změnu systému vyvážil. I přes toto špatné rozhodnutí se však dalo minimálně části zbytečně vynaložených nákladů zabránit tím, že by byl nakoupen pro pilotní provoz menší počet karet standardu MIFIRE Classic, případně by byly dle původních předpokladů dodrženy i propagační a marketingové aktivity, které předpokládaly vyšší rozšíření karet mezi uživatele již v pilotním provozu.

V průběhu roku 2007 došlo k nastavení smluvních podmínek tak, že bylo **proti zavedeným pravidlům a interním metodikám MHMP** umožněno proplácet faktury vystavené společností Haguess za provoz

kartového centra na počátku měsíce, v němž docházelo k plnění. Tento stav byl **v průběhu roku 2008 narovnán**.

Dne 13.9.2007 proběhl audit v centrálním pracovišti Haguess, provedený společností Relsie s.r.o. na základě objednávky MHMP. Tento audit byl zaměřen hlavně na technologické a bezpečnostní parametry systému. V obecné rovině **neshledal žádná fatální pochybení**, přesto však uvádí množství doporučení a námětů pro další postup HMP v projektu. V průběhu posouzení se nám podařilo získat informace o tom, že první kroky vycházející z doporučení Relsie s.r.o. byly ze strany HMP realizovány až v polovině roku 2008. Tato prodleva byla dle informací odboru Informatiky způsobena objektivně složitou situací ve vyjednávání změny podmínek se společností Haguess.

Dne 30.06.2008 byla uvedena do provozu nová verze systému SKC a KAP pracující s kartami MIFARE Classic i MIFARE DESFire. Dne 30.06.2008 byla předána nabídka společnosti Haguess na zakázku "Rozšíření SKC o MIFARE DESFire". Z toho plyne, že nová verze systému byla uvedena do provozu současně s podáním nabídky. Při zjišťování příčin tohoto postupu jsme dospěli k závěru, že spuštění nové verze systému SKC a KAP pravděpodobně souviselo s časovým tlakem ze strany dopravních podniků a spuštění dopravní aplikace, která měla podporu MIFARE DESFire ve svých podmínkách. Přesto se nám tuto informaci nepodařilo zcela zřetelně získat z projektové dokumentace, kde by měla být uvedena.

Dne 29.07.2008 proběhla za účasti zástupců HMP v centrálním pracovišti PCKS vzorová ukázka generování klíčů ke kartám MIFARE DESFire. Součástí této ukázky bylo předání přístupových karet k HSM SKC-Provoz a HSM-Záloha příslušným bezpečnostním úředníkům HMP. Za porušení bezpečnostních pravidel jsme vyhodnotili situaci, kdy ve stejný den zástupce HMP, Ing.Ivan Lukeš, pověřil zástupce Haguess, Ing.Vladimíra Valdu, aby jej zastupoval při importu klíčů a dále zástupce HMP, Ing.Ivan Seyček, pověřil zástupce Haguess, RNDr.Jana Kodovského, aby jej zastupoval při importu klíčů. Zodpovědní pracovníci MHMP se **tímto vzdávají jedné z možností kontrol**, případně možnosti podílet se na projektu. Tento stav narovnán až v průběhu roku 2008 a od tohoto okamžiku jsou „klíče" v rukách zodpovědných pracovníků MHMP.

Projekt „Servisního kartového centra" (taktéž PCMS „Prague Card Managemet System") byl vyhlášen zadáním veřejné zakázky na služby formou otevřeného řízení podle tehdy platného zákona č. 40/2004 Sb. o veřejných zakázkách. Realizace výběrového řízení **proběhla dle reguli zmiňovaného zákona** a dle interních metodik zadavatele MHMP.

Po revizi způsobu zadávání veřejných zakázek malého rozsahu v rámci projektu PCMS, lze říci, že tyto **zakázky byly v souladu s interními přepisy MHMP** a soutěženy mezi 3 subjekty (minimálně), a to v převážné většině prostřednictvím tzv. certifikovaného elektronického tržiště a nad rámec tohoto předpisu je veřejná zakázka již ve fázi vypsání zobrazena i na veřejné úřední desce MHMP (dle získaných údajů nejméně od roku 2008). Po věcné stránce byly veřejné zakázky malého rozsahu na

konzultační služby, na služby řízení projektu a na právní služby, zadávány zřejmě v návaznosti na aktuální vývoj projektu PCMS a jeho subprojektů.

Hlavní stávající a budoucí rizika projektu

Projekt sám o sobě nese v současné podobě množství rizik. Nejdůležitějšími z nich jsou:

- Riziko, že celé řešení nebude akceptováno uživateli (Pražany)
- Projektové řízení (2006-2007) probíhalo mimo odbor informatiky MHMP, bylo outsourcováno a současně se při řízení projektu vystřídalo několik společností bez dostatečně definovaných pravidel zodpovědnosti a jejich předávání/přebírání.
- Velkým rizikem projektu je zatím omezená funkcionalita karty (není multifunkční)
- Oproti původním očekáváním není zprovozněno plánované portfolio kartových aplikací
- Rizikem při zavedení byla dlouhá doba realizace k prvnímu „masovějšímu" rozšíření – roční předplatné MHD
- Významným rizikem pro rozvoj aplikací typu elektronická peněženka je fakt, že pro finanční služby nebyl získán významný finanční partner – banka, tím vzniká přenesený problém chybějící bankovní licence pro elektronickou peněženku a přináší nutnost řešení plateb pomocí výjimek.
- Součinnost DPP (ukončil participaci na projektu březen 2009)
- Rizikem projektu se stal i fakt, že DPP vyhlašoval vlastní výběrová řízení na činnosti související s projektem PCMS bez přímé koordinace s MHMP
- Projektovým rizikem je závislost MHMP na jednom exkluzivním dodavateli (Haguess)
- Při výběrových řízení typu JŘBU – jednací řízení bez uveřejnění, je nutné důkladně ověřovat obvyklost a přiměřenost sjednané ceny z nezávislých zdrojů.
- Výchozím rizikem projektu byl i fakt, že dodavatel (Haguess) neměl dle dostupných informací dostatečné reference v dané oblasti. Toto riziko se za dobu existence z technologického hlediska ukázalo jako neopodstatněné, přesto však mohou některé kroky v průběhu projektu souviset i s tímto rizikem
- Obecně jsou velkým rizikem podobných projektů formy bezpečnosti a to jak technické a technologické, tak z pohledu business kontinuity apod.
- Rizikem je i neexistence komplexního nástroje nebo metodiky řízení rizik, disaster & recovery plánu apod.
- Kromě rizik identifikovaných v rámci našeho posouzení je nutné zvážit další rizika zejména v oblasti ekonomického, licenčního a smluvního charakteru.

Doporučení pro další rozvoj

Vlastní projekt PCMS je postaven na obecně fungujících principech podobných řešení v ČR i v zahraničí a má vysoký potenciál dalšího využití, pokud bude ze strany MHMP nalezen vhodný ekonomický model.

Cílem projektu Opencard by mělo být vybudování identifikačního a platebního, multiaplikačního nástroje pro občany a návštěvníky HMP s podobným nebo ještě lépe vyšším rozsahem, jaký je obvyklý v moderních evropských i světových metropolích (například Oyster Card v Londýně, nebo Octopus Card v Hong Kongu).

Využití Opencard by mělo být zaměřeno hlavně do následujících oblastí:

- Technologické zázemí – hybridní karta, multiplikační centrum, platební a zúčtovací systém, elektronická peněženka – tzv. mikroplatby (mikropayment)
- Městské služby – knihovny, kultura, sport, školství
- Turistické aplikace – např. jednotlivé jízdné (SMS jízdenky fungují jen pro klienty českých operátorů), denní, trojdenní, týdenní, parkování, kultura, sport, služby, ubytování.
- Konferenční, kongresová a veletržní aplikace – identifikační karta, které slouží současně pro pobyt ve městě
- Dopravní infrastruktura – např. parkovací zóny, MHD, krátkodobé jízdné, mýtný systém.
- Městské utility – elektřina, voda, plyn, teplo, odpady
- Městské kontaktní centrum – portál města, přepážkový systém, terminály, čtečky, call centrum, městská policie
- Zdravotnictví – např. nemocnice, poliklinky, záchranná služba, sociální služby, soukromé ordinace.
- Komerční organizace – např. obchodní řetězce, restaurace, hotely, stravování pro zaměstnance, internet platby, benzínová čerpadla, prodejní automaty (káva, nápoje, občerstvení), kina, taxi.
- Kromě oblastí zpracovaných v rámci našeho posouzení doporučujeme vyhodnotit oblasti ekonomických a licenčních vztahů s partnery a jejich úzké součinnosti s HMP.

Jsme připraveni Zadavateli toto posouzení osobně prezentovat.

Děkuji a zůstávám s pozdravem!

V Praze dne 10.1.2010

Ing. Jiří Berger, MBA
Jednatel e-FRACTAL

Upozorňujeme, že jakékoliv použití informací uvedených v manažerském shrnutí bez kontextu kompletní zprávy, nemusí přesně vystihovat danou podstatu a stav jednotlivých částí projektu.

3. Rekapitulace projektu mezi HMP a Haguess

V rámci posouzení jsme provedli v součinnosti se zúčastněnými subjekty inventuru a časovou posloupnost celého projektu od jeho počátku až do 30.6.2009, aby existoval základ, na kterém je celé posouzení postaveno. Současné jsme provedli soupis všech informačních zdrojů, které nám byly zpřístupněny a z kterých jsme vycházeli.

3.1. Před zahájením projektu

Dne 23.12.2005 bylo na centrální adrese zveřejněno Předběžné oznámení vedené pod číslem 50015619. Název veřejné zakázky je Univerzální karta Pražana. Zakázka je stručně popsána takto: Dodávka musí pokrývat HW, SW technologie a služby nutné pro realizaci projektu UKP v následujících oblastech:
Městské kontaktní centrum, Dopravní infrastruktura, Městské služby, Distribuční sítě města, Komerční organizace, Turistické aplikace.

Předpokládané datum oznámení veřejné zakázky bylo 1.3.2006. Předpokládaná cena je 7.000.000 bez DPH na programové vybavení. Oprávněnou osobou za zadavatele je Ivan Seyček.

Dne 16.05.2006 rada HMP schválila svým usnesením číslo 0708 realizaci projektu Pražské centrum kartových služeb formou projektového portfolia s cílem zavést služby pro obyvatele a návštěvníky hl. m. Prahy.

Následně dne 28.06.2006 byla na centrální adrese zveřejněna Veřejná zakázka "Realizace Servisního Kartového Centra" vedená pod evidenčním číslem 50023676. Veřejná zakázka má povahu otevřeného řízení. Předpokládaný finanční objem je 66.000.000 bez DPH na informační systémy a 24.000.000 bez DPH na 50.000 ks karet. Doba plnění je od 1.10.2006 do 31.12.2011. Zadavatelem je Hlavní město Praha. Oprávněnou osobou k jednání jménem zadavatele je uveden I.Seyček. Kontaktní osobou je J.Chytil.

Stručný popis předmětu zakázky: Realizace Servisního Kartového Centra včetně služeb implementace dle požadavků zadavatele, zajištění následného provozu a podpory systému a dodávka hybridních čipových karet. Lhůta pro podání nabídky byla stanovena do 25.8.2006, 12 hod.

Dne 26.09.2006 rada HMP rozhodla na svém zasedání o přidělení veřejné zakázky na Realizaci SKC společnosti Haguess.

Dne 05.10.2006 bylo dopisem HMP doručeno rozhodnutí zadavatele č.j. MHMP/INF/1422/2006 o přidělení veřejné zakázky dle zákona č.40/2004. Zadavatel rozhodl o přidělení veřejné zakázky Realizace SKC společnosti Haguess.

3.2. Pilotní fáze projektu, projekt

3.2.1. Rok 2006

Datum	Fáze projektu
23.10.2006	Dne 23.10.2006 byla uzavřena smlouva mezi HMP a společností Haguess na zakázku Realizace SKC. Jedná se o smlouvu o dílo vedenou u objednatele pod číslem DIL/40/05/001120/2006 její nedílnou přílohou je Vzor Servisní smlouvy a Licenční smlouvy na KRONUS, QUANTO, KWADROM, CHANSON.
25.10.2006	Dne 25.10.2006 byly podepsány Podmínky realizace projektu SKC. Jedná se o dokument vydaný společností Soluziona, která byla dodavatelem služeb projektového řízení a zastřešovala tzv. projektové portfolio (dílčí realizační projekty) PCKS. Dokument definuje organizační podmínky, rozsah dodávky, složení projektových týmů a harmonogram projektu. Přílohou dokumentu jsou pak následující metodiky sdílené všemi dodavateli realizačních projektů PCKS: Metodika řízení projektu PCKS, Pravidla pro vedení projektové dokumentace projektu PCKS, Pravidla pro řízení rizik projektu PCKS, Pravidla pro řízení kvality projektu PCKS.
3.11.2006	Dne 03.11.2006 předal vedoucí projektového portfolia PCKS za společnost Soluziona oficiálně požadavky společnosti Haguess na součinnost HMP. Požadavky předal zástupci integrační kanceláře MHMP.
6.11.2006	Dne 06.11.2006 byla mezi HMP a společností Haguess uzavřena Licenční smlouva (LIC/40/05/001127/2006) na KRONUS, QUANTO, KWADROM, CHANSON.
8.11.2006	Dne 08.11.2006 předala na základě Licenční smlouvy (LIC/40/05/001127/2006) společnost Haguess zástupci HMP licenci Software SKC (Kronus, Quanto, Kwadrom, Chanson) na nosiči (DVD).
9.11.2006	Následně hned dne 09.11.2006 byla na základě smlouvy o dílo a předání licence Software SKC vystavena faktura č.FV-601156/2006 na částku 28.025.000 Kč bez DPH. Částka je součástí ceny za implementaci včetně dodávky HW a SW dle smlouvy DIL/40/05/001120/2006 a je vypočtena z parametrů uvedených zadání zakázky (Realizace SKC) a dle licenčního modelu uvedeného ve vzoru licenční

	smlouvy, který byl součástí nabídky společnosti, je i součástí podepsané smlouvy ze dne 23.10.2006 a je uveden ve smlouvě LIC/40/05/001127/2006.
4.12.2006	Ke dni 04.12.2006 byly předány k připomínkování: Specifikace řešení kartové aplikace Čtenářský průkaz do Městské knihovny a Specifikace řešení kartové aplikace Bezhotovostní úhrada parkování. Dokumenty byly zaslány mailem na členy koncepční skupiny PCKS v souladu s řídícími dokumenty projektového portfolia PCKS a zápisy z jednání koncepční skupiny.
5.12.2006	Dne 05.12.2006 byla přijata žádost ředitele odboru Informatiky HMP č.j. MHMP/INF/1928/2006 o zajištění kurýrní služby pro přepravu personalizovaných karet na kontaktní místa ve Škodově paláci v souladu s požadavky uvedenými v nabídce řešení SKC a v odsouhlaseném prováděcím projektu. Součástí žádosti je i žádost o dodání návrhu smlouvy (smluv), které budou specifikovat podmínky poskytnutí požadovaných služeb.
5.12.2006	Dne 05.12.2006 byla přijata žádost ředitele odboru informatiky HMP č.j. MHMP/INF/1927/2006 o zajištění prostor technického zázemí SKC a personalizační linky, včetně personálního zajištění jejich provozu v souladu s požadavky uvedenými v nabídce řešení SKC a odsouhlaseném prováděcím projektu. Součástí dopisu je i žádost o dodání návrhu smlouvy (smluv), které budou specifikovat podmínky poskytnutí požadovaných služeb (SLA).
7.12.2006	Dne 07.12.2006 předala na základě Smlouvy o dílo (DIL/40/05/001120/2006) společnost Haguess zástupci HMP 1. část HW pro realizaci SKC (Stanice Dell, 10.000ks čteček kontaktního čipu karet). Byl podepsán předávací protokol. Současně byla na základě smlouvy o dílo a předání 1. části HW pro realizaci SKC byla vystavena faktura č. FV-601158/2006 na částku 3.566.870 Kč bez DPH. Částka je součástí ceny za implementaci včetně dodávky HW a SW dle smlouvy DIL/40/05/001120/2006.
8.12.2006	Dne 08.12.2006 byla zástupcem Městské knihovny Praha odsouhlasena Specifikace řešení kartové aplikace Čtenářský průkaz do Městské knihovny v Praze.

11.12.2006	Dne 11.12.2006 byla předána k připomínkování Specifikace řešení kartové aplikace Přístup na portál HMP s využitím Opencard. Dokument byl zaslán mailem na členy koncepční skupiny PCKS v souladu s řídícími dokumenty projektového portfolia PCKS a zápisy z jednání koncepční skupiny.
12.12.2006	Dne 12.12.2006 bylo společností Haguess přijato vyjádření Odboru dopravy MHMP č.j. MHMP-463759/2006/DOP/RD/P1 ke Specifikaci řešení kartové aplikace Parkování.
15.12.2006	Dne 15.12.2006 byla odsouhlasena zástupcem Odboru dopravy MHMP Specifikace řešení kartové aplikace bezhotovostní úhrady parkování s využitím čipové karty "Opencard". Současně byla odsouhlasena zástupcem Odboru informatiky MHMP Specifikace řešení přístupu na Portál HMP s využitím čipové karty "Opencard". Ve stejný den předala společnost Haguess na základě Smlouvy o dílo (DIL/40/05/001120/2006) zástupci HMP Serverovou část SKC (cena bez DPH 4.090.731 Kč), Licenci DBS Oracle (cena bez DPH 1.137.887 Kč) a SW licenci pro HSM (cena bez DPH 1.097.685 Kč). Uvedené částky jsou součástí předávacího protokolu. Na základě smlouvy o dílo a předání Serverové části SKC, Licence DBS Oracle a SW licence pro HSM byla vystavena faktura č. FV-601159/2006 na částku 6.326.303 Kč bez DPH. Částka je součástí ceny za implementaci včetně dodávky HW a SW dle smlouvy DIL/40/05/001120/2006.
19.12.2006	Dne 19.12.2006 byla vystavena zálohová faktura č. DZV-1/2006 na částku 11.750.000 bez DPH.

3.2.2. Rok 2007

Datum	Fáze projektu
15.1.2007	Dne 15.01.2007 byla předána k připomínkování Specifikace řešení SKC. Dokument byl zaslán mailem na členy koncepční skupiny PCKS v souladu s řídícími dokumenty projektového portfolia PCKS a zápisy z jednání koncepční skupiny.
1.2.2007	Dne 01.02.2007 byla ukončena akceptace Specifikace řešení Kartových aplikací podepsáním akceptačního protokolu.
1.2.2007	Dne 01.02.2007 byla v návaznosti na veřejnou zakázku Realizace SKC doručena Výzva č.j. INF/213/2007 k jednání v jednacím řízení bez uveřejnění na realizaci veřejné zakázky "Realizace KAP" pro HMP. Uvedená doba plnění je do 31.12.2009.
8.2.2007	Na základě smlouvy o dílo DIL/40/05/001120/2006 a akceptace Specifikace řešení Kartových aplikací byla dne 08.02.2007 vystavena faktura č. FV-4/2007 na částku 950.000 Kč bez DPH. Částka je součástí ceny za návrh funkčního řešení SKC a návrh funkčního řešení KA dle smlouvy DIL/40/05/001120/2006.
15.2.2007	Dne 15.02.2007 bylo doručeno oznámení č.j. INF/377/2007 o výběru nejvhodnější nabídky v jednacím řízení bez uveřejnění na Kartovou aplikaci parkování pro HMP.
26.2.2007	Dne 26.02.2007 byla uzavřena smlouva o dílo č. INO/40/05/001270/2007 na Realizaci KAP za celkovou cenu 8.880.095 Kč bez DPH. Na základě této smlouvy byla zavřena licenční smlouva č. LIC/40/05/001272/2007 na Software KAP. Smlouva na straně 6 definuje Software KAP jako aplikaci, která je funkčně i datově provázána s moduly aplikačního Software SKC. KAP bude využívat smlouvou definované funkce Chanson (back-office elektronické peněženky) a Kwadrom (zúčtovací systém). Dále byla na základě smlouvy č. INO/40/05/001270/2007 uzavřena servisní smlouva č. DIL/40/05/001271/2007 na Software KAP po dobu 2 let v celkové ceně 1.170,00 Kč bez DPH.
1.3.2007	Dne 01.03.2007 byla v návaznosti na veřejnou zakázku Realizace SKC byla doručena Výzva č.j. INF/424/2007 k jednání v jednacím řízení bez uveřejnění na realizaci

	veřejné zakázky "Rozšířené zajištění provozních činností PCKS po dobu zkušebního provozu" pro HMP. Doba plnění je do 30.9.2007.
5.3.2007	Dne 05.03.2007 předala společnost Haguess na základě smlouvy INO/40/05/001270/2007 (a smlouvy LIC/40/05/001272/2007) zástupci HMP licenci KAP. Následně byla na základě Smlouvy č. INO/40/05/001270/2007 a na základě předávacího protokolu ze dne 5.3.2007 vystavena faktura č.FV-6/2007 za licenci KAP pro 50.000 držitelů karet a 150 ks parkovacích automatů ve výši 1.613.500 Kč bez DPH.
8.3.2007	08.03.2007 Na základě Smlouvy o dílo (DIL/40/05/001120/2006) předal Haguess zástupci HMP 2.část HW (periférie) v ceně 471.431 Kč bez DPH. Uvedená částka je součástí předávacího protokolu. Faktura FV-7/2007 byla vystavena 16.3.2007.
12.3.2007	Dne 12.03.2007 byla v návaznosti na veřejnou zakázku Realizace SKC byla doručena Výzva č.j. INF/481/2007 k jednání v jednacím řízení bez uveřejnění na realizaci veřejné zakázky "Portálové řešení Univerzální karty Pražana" pro HMP. Doba plnění je do 31.12.2007.
19.3.2007	Dne 19.03.2007 byl podepsán akceptační protokol a tím byla ukončen proces akceptace aplikačního software SKC v souladu se smlouvou DIL/40/05/001120/2006. Byla vystavena faktura č. FV-8/2007 na částku 3.618.482 Kč bez DPH a faktura č. FV-9/2007 na částku 1.100.000 Kč bez DPH.
19.3.2007	Dne 19.03.2007 Požádala společnost Haguess dopisem HMP dopis s žádostí o posun termínu na předložení nabídky na realizaci veřejné zakázky "Portálové řešení UKP" pro HMP o 14 dnů. Výzva k podání nabídky je vedena pod č.j. INF/481/2007.
20.3.2007	Dne 20.03.2007 Na základě Smlouvy o dílo (DIL/40/05/001120/2006) předala společnost Haguess zástupci HMP 50.000 ks hybridních produktově personalizovaných čipových karet GemTwin. Související faktura č. FV-10/2007 na částku 4.092.160 Kč bez DPH byla vystavena dne 10.04.2007. Fakturovaná cena je rozdílem částky 15.842.160 - 11.750.000 (záloha poskytnutá objednatelem v roce 2006).

23.3.2007	Dne 23.03.2007 bylo doručena oznámení č.j. INF/539/2007 o výběru nejvhodnější nabídky na zakázku Rozšířené zajištění provozních činností PCKS po dobu zkušebního provozu.
27.3.2007	Dne 27.03.2007 bylo doručeno oznámení č.j. INF/597/2007 o výběru nejvhodnější nabídky na zakázku Rozšířené zajištění provozních činností PCKS po dobu zkušebního provozu.
12.4.2007	Dne 12.04.2007 byla uzavřena smlouva o zajištění provozu PCKS č. INO/40/05/001296/2007 na období od 1.4.2007 do 30.9.2007. V návaznosti na tuto smlouvu byla uzavřena mandátní smlouva č. MAN/40/05/001297/2007 a dále byla uzavřena smlouva č. INO/40/05/001298/2007 o zpracování osobních údajů. V souladu s přílohou č.3 smlouvy INO/40/05/001270/2007 předal zástupce Haguess zástupci HMP 1. soubor upravených parkovacích automatů.
22.6.2007	Dne 22.06.2007 byla v souladu se smlouvou č. INO/40/05/001296/2007 vystavena faktura č. FV-23/2007 na období 1.6.2007 - 30.6.2007. Dne 24.07.2007 byla vystavena faktura č. FV-26/2007 na období 1.7.2007 - 31.7.2007. Dne 17.8.2007 byla vystavena faktura č. FV-27/2007 na období 1.8.2007 - 31.8.2007.
13.9.2007	Dne 13.09.2007 probíhl audit v centrálním pracovišti Haguess Na Sychrově 8, Praha 10 provedený společností Reisle s.r.o. na základě objednávky MHMP.
17.9.2007	Dne 17.09.2007 byla v souladu se smlouvou č. INO/40/05/001296/2007 vystavena faktura č. FV-29/2007 na částku 2 074 159,00 za období 1.9.2007 - 30.9.2007.
24.9.2007	Dne 24.09.2007 bylo uzavřeno několik dodatků k předchozím smlouvám, konkrétně: • dodatek č. 1 ke smlouvě č. INO/40/05/001296/2007 o zajištění provozu PCKS. • dodatek č. 1 ke smlouvě č. MAN/40/05/001297/2007 o vydávání a správě karet Opencard. • dodatek č.1 ke smlouvě č. INO/40/05/001298/2007 o zpracování osobních údajů. • O dva dny později byl uzavřen dodatek č. 2 ke

	smlouvě č. INO/40/05/001296/2007 o zajištění provozu PCKS, kterým se mimo jiné prodlužuje zkušební provoz KAP do 31.10.2007.
30.9.2007	Dne 30.09.2007 zástupce společnosti Haguess předal zástupci HMP zprávu o vyhodnocení zkušebního provozu SKC (12.4.-30.9.2007) a předložil akceptační protokol, čímž byl ukončen zkušební provoz SKC v souladu se smlouvou DIL/40/05/001120/2006. Na základě akceptace byla vystavena faktura č. FV-30/2007 na částku 3.961.320 Kč bez DPH za poimplementační podporu SKC-zajištění zkušebního provozu.
11.10.2007	Dne 11.10.2007 byla přijata výzva k jednání v jednacím řízení bez uveřejnění č.j. INF/1701/2007 na zakázku Zajištění provozních činností PCKS.
15.10.2007	Dne 15.10.2007 byla v souladu se smlouvou č. INO/40/05/001296/2007 a jejími dodatky 1 a 2 vystavena faktura č. FV-32/2007 na částku 2 817 709,90 za období 1.10.2007 - 30.10.2007.
16.10.2007	Dne 16.10.2007 byla předána odboru informatiky nabídka společnosti na zakázku "Provoz PCKS". 16.10.2007 bylo přijato Oznámení o výběru nejvhodnější nabídky č.j. INF/1713/2007 na zakázku "Zajištění provozních činností PCKS".
31.10.2007	Dne 31.10.2007 byla doručena objednávka od MHMP č.j. MHMP/INF/1815/2007 ze dne 25.10.2007 na "Vytvoření podkladů pro rozšíření Kartové Aplikace Parkování do nově zřizovaných zón placeného stání HMP".
31.10.2007	Dne 31.10.2007 byla uzavřena smlouva o zajištění provozu PCKS č. INO/40/01/001386/2007 na období 1.11.2007-31.7.2008 a v návaznosti na smlouvu o zajištění provozu PCKS č. INO/40/01/001386/2007 byla uzavřena mandátní smlouva č. MAN/40/01/001387/2007. V návaznosti na mandátní smlouvu MAN/40/01/001387/2007 a smlouvu o zajištění provozu PCKS č. INO/40/01/001386/2007 byla uzavřena smlouva č. INO/40/01/001388/2007 o zpracování osobních údajů.
14.11.2007	Dne 14.11.2007 byla na základě smlouvy o zajištění provozu PCKS č. INO/40/01/001386/2007 z 31.10.2007 vystavena faktura č. FV-33/2007 na částku 1 695 757,00 za období 1.11.2007 - 30.11.2007.

15.11.2007	Dne 15.11.2007 byla předána dokumentace "Podklady pro rozšíření Kartové Aplikace Parkování do nově zřizovaných zón placeného stání Hlavního města Prahy" v souladu s objednávkou HMP č.j. MHMP/INF/1815/2007 ze dne 25.10.2007. Faktura za tuto činnost byla vystavena 22.11.2007 pod č. FV-37/2007 na částku 187.000 Kč bez DPH.
18.11.2007	Dne 18.11.2007 byla na základě uplynutí zkušebního provozu KAP (po dobu 6 měsíců od 18.5.2007) v souladu se smlouvou č. INO/40/05/001270/2007 vystavena faktura č. FV-35/2007 na částku 505.100 Kč bez DPH.
30.11.2007	Dne 30.11.2007 byla vystavena na základě smlouvy č. DIL/40/05/001120/2006 faktura č. FV-39/2007 na částku 4 591 555,00 za servisní období 1.11.2007 - 31.10.2008 k licenci Software SKC.
3.12.2007	Dne 03.12.2007 byla na základě smlouvy o zajištění provozu PCKS č. INO/40/01/001386/2007 z 31.10.2007 vystavena faktura č. FV-38/2007 na částku 1 695 757,00 za období 1.12.2007 - 31.12.2007.

3.3. Vydávání karet pro veřejnost (2007).

Datum	Činnost
12.4.2007	Dne 12.04.2007 byl zahájen provoz PCKS pro veřejnost. Příjem žádostí o vydání Opencard zajišťují 4 přepážky v paláci Adria provozované společností Haguess (obsluhu přepážky tvoří zaměstnanci společnosti).
16.4.2007	Dne 16.04.2007 byla na základě smlouvy INO/40/05/001270/2007 a na základě předání 1. souboru upravených parkovacích automatů vystavena faktura č. FV-12/2007 na částku 1.271.996 Kč bez DPH.
23.4.2007	Dne 23.04.2007 byla v souladu se smlouvou č. INO/40/05/001296/2007 byla vystavena faktura č. FV-13/2007 na období 12.4.2007 - 30.4.2007.
26.4.2007	Dne 26.04.2007 předal v souladu s přílohou č.3 smlouvy INO/40/05/001270/2007 zástupce Haguess zástupci HMP 2. soubor upravených parkovacích automatů a byla vystavena faktura č. FV-14/2007 na částku 1.271.996 Kč bez DPH.
30.4.2007	Dne 30.04.2007 předal v souladu s přílohou č.3 smlouvy INO/40/05/001270/2007 zástupce Haguess zástupci HMP 3. soubor upravených parkovacích automatů a byla vystavena faktura č. FV-15/2007 na částku 1.271.996 Kč bez DPH.
10.5.2007	Dne 10.05.2007 byl v souladu s přílohou č.3 smlouvy INO/40/05/001270/2007 předán společností Haguess zástupci HMP 4. soubor upravených parkovacích automatů a byla vystavena faktura č. FV-16/2007 na částku 1.271.996 Kč bez DPH.
15.5.2007	Dne 15.05.2007 byla v souladu se smlouvou č. INO/40/05/001296/2007 byla vystavena faktura č. FV-18/2007 na částku 2 074 159,00 na období 1.5.2007 - 31.5.2007.
18.5.2007	Dne 18.05.2007 předal v souladu s přílohou č.3 smlouvy INO/40/05/001270/2007 zástupce Haguess zástupci HMP 5. soubor upravených parkovacích automatů a byla vystavena faktura č. FV-19/2007 na částku 1.271.996 Kč bez DPH. V souladu s přílohou č.2 smlouvy INO/40/05/001270/2007 předal zástupce společnosti Haguess zástupci HMP také HW a SW v

	celkové hodnotě 401.515 Kč bez DPH. Součástí předávacího protokolu jsou jednotkové (kusové) ceny jednotlivých předávaných položek.
24.5.2007	Dne 24.05.2007 byla na základě smlouvy INO/40/05/001270/2007 a na základě předávacího protokolu ze dne 18.5.2007 vystavena faktura č.FV-17/2007 na dílčí předávané části v celkové ceně 83.452 Kč bez DPH faktura č.FV-20/2007 na dílčí předávané části v celkové ceně 260.581,2 Kč bez DPH, faktura č.FV-21/2007 na dílčí předávané části v celkové ceně 27.604,5 Kč bez DPH a faktura č.FV-22/2007 na dílčí předávané části v celkové ceně 29.876,07 Kč bez DPH.

3.4. Útok na karetní technologii (2007).

Datum	Činnost
12.6.2007	Dne 12.06.2007 byl proveden útok společností Iuridicum Remedium na kartu Opencard a proběhla veřejná demonstrace čtení osobních údajů z karty. Následující den byla jako reakce na tuto událost a dále za účelem eliminace rizika poškození karty a možného poškození projektu Opencard, přijata společností Haguess, a.s. následující opatření: • Údaje o držiteli karty uložené v rámci procesu personalizace v elektronické podobě do prvního sektoru bezkontaktního čipu MIFARE Classic 4kB jsou při kontrole výstupů personalizační linky z karty vymazány. • Pro již vydané karty byla zavedena možnost vymazání údajů na kontaktním místě buď na přímou žádost držitele karty, nebo automaticky při nabití parkovacího kupónu.
31.8.2007	Dne 31.08.2007 byla na základě žádosti HMP ze dne 30.8.2007 předána zástupcem společnosti Haguess zástupci HMP Provozní dokumentace PCKS (popisy pracovních postupů a provozní řád) a to za účelem jednání HMP s Úřadem pro ochranu osobních údajů.
7.9.2007	Dne 07.09.2007 předal zástupce společnosti Haguess zástupci HMP dokumentaci k systému SKC v rozsahu Datová komunikace se systémy kartových aplikací a Webové služby (oba dokumenty popisují otevřené datové rozhraní systému SKC první z pohledu dávkové komunikace druhý z pohledu on-line komunikace), Bezpečnostní politika systému SKC.
10.9.2007	Dne 10.09.2007 předal zástupce Haguess zástupci HMP dokumentaci k systému SKC v rozsahu Specifikace řešení SKC a Specifikace řešení SKC - Prováděcí projekt systému SKC a KAP, verze 1.5.

3.4.1. Rok 2008

Datum	Fáze projektu
7.1.2008	Dne 07.01.2008 byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS vystavena faktura č. FV-1/2008 na 1 866 097,00 Kč za období 1.1.2008-31.1.2008.
31.1.2008	Dne 31.01.2008 byla v souladu se smlouvou č. DIL/40/05/001271/2007 vystavena faktura č. FV-4/2008 na částku 146 250,00 za servisní podporu informačního systému KAP (v období 1.11.2007-31.1.2008).
1.2.2008	Dne 01.02.2008 byla doručena Výzva k podání nabídky a k prokázání splnění kvalifikace v rámci zjednodušeného podlimitního řízení č.j. INF/132/2008 ze dne 29.1.2008.
4.2.2008	Dne 04.02.2008 byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS byla vystavena faktura č.FV-7/2008 na částku 1 866 097,00 Kč za období 1.2.2008-29.2.2008.
20.2.2008	Dne 20.02.2008 byl uzavřen dodatek č.1 ke smlouvě č.INO/40/01/001388/2007 o zpracování osobních údajů.
4.3.2008	Dne 04.03.2008 byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS vystavena faktura č.FV-12/2008 za období 1.3.2008-31.3.2008 na částku 1 866 097 Kč.
13.3.2008	Dne 13.03.2008 bylo doručeno "Oznámení o výběru nejvhodnější nabídky" na realizaci veřejné zakázky "Kartová aplikace Parkování v nových zónách placeného stání" zahájené 29.1.2008 odesláním výzvy č.j. INF/132/2008. Druhou ekonomicky nejvýhodnější nabídkou byla nabídky fy. TELMAX, s.r.o. Třetí nabídky f. XT-Card, a.s. byla ze zadávacího řízení vyloučena.
1.4.2008	Dne 01.04.2008 byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS byla vystavena faktura č.FV-15/2008 za období 1.4.2008-30.4.2008 na částku 1 866 097 Kč.
21.4.2008	Dne 21.04.2008 byla uzavřena smlouva na KAP II vedená u HMP pod číslem DIL/40/01/001529/2008 za celkovou cenu 4.695.920 Kč bez DPH.

25.4.2008	Dne 25.04.2008 předal zástupce společnosti Haguess na základě smlouvy OIL/40/01/001529/2008 zástupci HMP "Licenci kartové aplikace parkování II" (D.V.6.b). Společně s předáním proběhlo i předání jednotlivých položek HW a SW včetně souvisejících služeb a na základě předání licence KAPII byla vystavena faktura č. FV-17/2008 na částku 2.912.200 Kč bez DPH. Současně na základě předání položek HW a SW byla vystavena faktura č. FV-18/2008 na částku 550.000 Kč bez DPH.
28.4.2008	Dne 28.04.2008 byla uvedena do provozu nová verze systému SKC a KAP (verze 2008).
5.5.2008	Dne 05.05.2008 byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS byla vystavena faktura č.FV-22/2008 za období 1.5.2008-31.5.2008na částku 1 866 097 Kč.
30.5.2008	Dne 30.05.2008 byla doručena Výzva č.j. INF/623/2008 k jednání v jednacím řízení bez uveřejnění na realizaci veřejné zakázky "Rozšíření licence Software SKC" pro HMP v návaznosti na veřejnou zakázku Realizace SKC. • Výzva INF/623/2008 30.5.2008 „JŘBU" – viz vyjádření legislativy z předchozích JŘBU na HGS. • Příloha č.1 - Zadávací dokumentace (předpokládaná cena 16mio bez DPH) licence typu A.I.1 (špatné označení, má být B.I.1) • Příloha č.1A – Požadavky na řešení • Jednání 12.6.2008, 13:00–14:05, Jungmannova, P1. Protokol. • Prokázání základních a profesních kvalifikačních předpokladů. • Nabídku podat do 15.6.2008, do 12:00 dle výzvy • Předávací protokol nabídky HGS 17.6.2008, je později dle dohody z 12.6.08, zaprotokolován. • Oznámení o výběru 24.6.2008 INF/738/2008 • Nabídka z 9.6.2008 před jednáním 12.6.08 a je úředně ověřená a také dne 9.6.2008. Avšak oba návrhy smluv jsou podepsané k 10.6.2009. • Licenční smlouva na „SAM" LIC/40/01/001650/2008 • Licenční smlouva na SKC 200 tis, 45 stanic, 5 aplikací.
2.6.2008	Dne 02.06.2008 byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS byla vystavena faktura č.FV-25/2008 za období 1.6.2008-30.6.2008 na částku 1 866 097 Kč.

4.8.2008	04.08.2008 V souladu se smlouvou č. DIL/40/05/001271/2007 byla vystavena faktura č. FV-34/2008 na servisní podporu informačního systému KAP. Faktura FV-34/2008 146 250,00.
14.8.2008	14.08.2008 Provedena příprava na integrační testy čtecích zařízení přepravních kontrolorů DPP na úrovni vytvoření transportního klíče mezi HSM SKC-Provoz a HSM testovacího prostředí. Vytvořený klíč byl použit pro následné načtení autentizačního klíče SAM revizora. Zápis je součástí akceptačního protokolu č.1 ze dne 14.10.2008 Zápis o vytvoření a vymazání transportního testovacího klíče.
15.8.2008	15.08.2008 V souladu se smlouvou o dílo č. DIL/40/01/001652/2008 byly formálně ukončeny služby sestavení HSM, jeho zprovoznění v infrastruktuře SKC a KAP a služby zavedení kryptografických klíčů. Protokol je součástí akceptačního protokolu č.1 ze dne 14.10.2008 Protokol o zprovoznění HSM a zavedení kryptografických klíčů.
18.8.2008	Dne 18.08.2008 dle licenční smlouvy č. LIC/40/01/001650/2008 předal zástupce společnosti Haguess zástupci HMP licenci Software SAM, dle licenční smlouvy č. LIC/40/01/001651/2008 licenci ASW HSM-SKC a byla vystavena faktura č. FV-37/2008 na licenci ASW HSM-SKC ve výši 1.100.000 Kč a licenci software SAM ve výši 645.840 Kč.
29.8.2008	Dne 29.08.2008 byly formálně uzavřeny všechny dodávky jednotlivých SAM a karet uživatelů SKC a KAP včetně provedení jejich inicializace. Protokol je součástí akceptačního protokolu č.1 ze dne 14.10.2008.
1.9.2008	Dne 01.09.2008 byla v souladu se smlouvou č. INO/40/01/001638/2008 ze dne 31.7.2008 o Zajištění provozu PCKS vystavena faktura č. FV-39/2008 za období 1.8.2008-31.8.2008 na částku 3 998 214 Kč.
10.9.2008	Dne 10.09.2008 byly dokončeny formálně úpravy parkovacích automatů v ZPS o položky umožňující akceptaci karet MIFARE DESFire dle smlouvy o dílo č. DIL/40/01/001652/2008. Protokol je součástí akceptačního protokolu č.1 ze dne 14.10.2008.
12.9.2008	Dne 12.09.2008 byly dokončeny a formálně předány úpravy kontaktního místa SKC o položky rozšiřující SKC (a KAP) o technologii MIFARE DESFire dle smlouvy o dílo č. DIL/40/01/001652/2008. Protokol je součástí akceptačního protokolu č.1 ze dne 14.10.2008, dále

	byly formálně uzavřeny všechny úpravy back-office SKC. Protokol je součástí akceptačního protokolu č.2 ze dne 18.11.2008 a zástupce společnosti Haguess formálně předal zástupci HMP 6 ks čteček pro práci s kartami MIFARE DESFire dle smlouvy o dílo č. DIL/40/01/001652/2008. Protokol je součástí akceptačního protokolu č.2 ze dne 18.11.2008.
29.9.2008	Dne 29.09.2009 byla uvedena do provozu nová verze systému SKC obsahující úpravy a nové funkce související zejména s podporou odbavování velkého počtu zájemců o kartu a zabezpečením komunikace s externí personalizační linkou.
1.10.2008	Dne 01.10.2008 byla v souladu se smlouvou č. INO/40/01/001638/2008 ze dne 31.7.2008 o Zajištění provozu PCKS vystavena faktura č. FV-46/2008 za období 1.9.2008-30.9.2008 ve výši 3 998 214 Kč.
13.10.2008	Dne 13.10.2008 proběhl akceptační test rozšíření SKC (a KAP) o technologii MIFARE DESFire dle testovacího scénáře. Test provedl zástupce HMP za účasti zástupce Haguess. Protokol je součástí akceptačního protokolu č.1 ze dne 14.10.2008.
14.10.2008	Dne 14.10.2008 byla v souladu s licenční smlouvou č. LIC/40/01/001651/2008 předána zástupcem společnosti Haguess zástupci HMP dokumentace k ASW HSM-SKC. Protokol je součástí akceptačního protokolu č.1 ze dne 14.10.2008 Současně byla ukončena formálně první část akceptace úprav SKC (a KAP) dle smlouvy o dílo DIL/40/01/001652/2008 podpisem akceptačního protokolu č.1.
16.10.2008	Dne 16.10.2008 byla na základě smlouvy č.DIL/40/01/001652/2008 ze dne 31.7.2008 a ukončení první části akceptace úprav SKC (a KAP) vystavena faktura č. FV-62/2008 za rozšíření back-office KAP (2.094.900 Kč), Úpravy PA v ZPS Praha 1 (5.353.200 Kč), Dodávku HSM a SAM (1.120.800 Kč), Úpravy kontaktních míst SKC (1.080.500 Kč). Celková částka faktury FV-62/2008 je9 649 400 Kč.
20.10.2008	Dne 20.10.2008 byla uzavřena smlouva č. DIL/40/01/001684/2008 o umožnění provozování kartové aplikace s využitím karty Opencard mezi HMP, jakožto garantem a vydavatelem karty, a DPP, jakožto provozovatelem kartové aplikace DOS. Garant umožňuje provozovateli přístup k PCKS a využít možnosti karty Opencard.

1.11.2008	Dne 01.11.2008 byla v souladu se smlouvou č. INO/40/01/001638/2008 ze dne 31.7.2008 o Zajištění provozu PCKS vystavena faktura č. FV-67/2008 za období 1.10.2008-31.10.2008 na částku 3 998 214,50 Kč.
10.11.2008	Dne 10.11.2008 byla v souladu se smlouvou č. DIL/40/05/001271/2007 byla vystavena faktura č. FV-68/2008 na servisní podporu informačního systému KAP na částku 146 250 Kč.
18.11.2008	Dne 18.11.2008 byla formálně ukončena druhá část akceptace úprav SKC (a KAP) dle smlouvy o dílo DIL/40/01/001652/2008 podpisem akceptačního protokolu č.2. Současně byla na základě smlouvy č.DIL/40/01/001652/2008 ze dne 31.7.2008 a ukončení druhé části akceptace úprav SKC vystavena faktura č. FV-70/2008 za úpravu interní personalizační linky SKC a úpravu back-office SKC na částku 4 562 100 Kč.
20.11.2008	Dne 20.11.2008 byla doručena výzva č.j. INF/1636/2008 k jednání v jednacím řízení bez uveřejnění na zakázku "Zajištění provozu PCKS v období 1.1.2009 - 28.2.2009".
30.11.2008	Dne 30.11.2008 byla v souladu se smlouvou č. DIL/40/05/001120/2006 ze dne 23.10.2006 vystavena faktura č. FV-77/2008 na servisní poplatek k licenci software SKC v období 1.11.2008-31.12.2008 ve výši 765 259 Kč.
1.12.2008	Dne 01.12.2008 byla v souladu se smlouvou č. INO/40/01/001638/2008 ze dne 31.7.2008 o Zajištění provozu PCKS vystavena faktura č. FV-75/2008 za období 1.11.2008-30.11.2008 na částku 3 998 214,50 Kč.
2.12.2008	Dne 02.12.2008 proběhlo 1 jednání v jednacím řízení bez uveřejnění k zakázce "Zajištění provozu PCKS v období 1.1.2009 - 28.2.2009"
4.12.2008	Dne 04.12.2008 byla v souladu se smlouvou č. DIL/40/05/001120/2006 ze dne 23.10.2006 vystavena faktura č. FV-77/2008 na servisní poplatek k licenci software SKC v období 1.1.2009-31.10.2009 na částku 3 826 295,80 Kč.
16.12.2008	Dne 16.12.2008 proběhlo druhé jednání v jednacím řízení bez uveřejnění na zakázku "Zajištění provozu PCKS v období 1.1.2009 - 28.2.2009".

17.12.2008	Dne 17.12.2008 proběhlo v souladu se smlouvou č. DIL/40/01/001529/2008 Licence kartové aplikace parkování KAP II" byla vystavena faktura č.FV-82/2008 za dodávku 298 ks SAM modulů na částku 1 233 720 Kč.
19.12.2008	Dne 19.12.2008 bylo doručeno oznámení č.j. INF/1854/2008 o výběru nejvhodnější nabídky na zakázku "Zajištění provozu PCKS v období 1.1.2009 - 28.2.2009".
31.12.2008	Dne 31.12.2008 byla v souladu se smlouvou č. INO/40/01/001638/2008 ze dne 31.7.2008 o Zajištění provozu PCKS vystavena faktura č. FV-85/2008 za období 1.12.2008-31.12.2008 na částku 3 998 214,50 Kč.

3.5. Změna karetní technologie

Datum	Činnost
30.5.2008	Dne 30.05.2008 byla doručena Výzva č.j. INF/622/2008 k jednání v jednacím řízení bez uveřejnění na realizaci veřejné zakázky "Rozšíření SKC o technologii MIFARE DESFire" pro HMP v návaznosti na veřejnou zakázku Realizace SKC.
12.6.2008	Dne 12.06.2008 proběhlo 1 jednání v jednacím řízení bez uveřejnění k zakázce Rozšíření licence Software SKC. Protokol o jednání.
24.6.2008	Dne 24.06.2008 bylo doručeno oznámení č.j. INF/738/2008 o výběru nejvhodnější nabídky na Rozšíření licence software SKC.
30.6.2008	Dne 30.06.2008 byla uvedena do provozu nová verze systému SKC a KAP pracující s kartami MIFARE Classic i MIFARE DESFire.
30.6.2008	Dne 30.06.2008 Předána nabídka společnosti Haguess na zakázku "Rozšíření SKC o MIFARE DESFire". Nabídka předána.
3.7.2008	Dne 03.07.2008 bylo přijato oznámení č.j. INF/806/2008 o výběru nejvhodnější nabídky v jednacím řízení bez uveřejnění na zakázku Rozšíření SKC o technologii MIFARE DESFire.
3.7.2008	Dne 03.07.2008 byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS byla vystavena faktura č.FV-28/2008 za období 1.7.2008-31.7.2008 na částku 1 866 097 Kč.
4.7.2008	Dne 04.07.2008 byla doručena výzva č.j. INF/805/2008 k jednání v jednacím řízení bez uveřejnění na zakázku Provoz PCKS v období od 1.8.2008 do 31.7.2009.
14.7.2008	Dne 14.07.2008 byla uzavřena licenční smlouva č.LIC/40/01/001613/2008 na rozšíření licence software SKC. Ve stejný den na základě této smlouvy předal zástupce společnosti Haguess zástupci HMP oprávnění k výkonu práva užít Software SKC v licenci typu C.III.1. (resp. maximální počet evidovaných karet 200.000, maximální počet uživatel.terminálů 45, maximální počet kartových aplikací 5). Oprávnění bylo uděleno formou písemného certifikátu. Současně byla vystavena

	faktura č.FV-31/2008 ve výši 14 610 000,00 za poskytnutí rozšíření licence SKC.
15.7.2008	Dne 15.07.2008 byla doručena Výzva k podání nabídky a k prokázání splnění kvalifikace dle par.38 odst 1 zákona č.137/2006 Sb. o veřejných zakázkách, ve znění zákona č. 110/2007 Sb. - zjednodušené podlimitní řízení na zakázku Výroba, produktová personalizace a dodávka čipových karet.
22.7.2008	Dne 22.07.2008 bylo přijato Oznámení o výběru nejvhodnější nabídky č.j. INF/920/2008 na zakázku "Provoz Pražského Centra Kartových Služeb"
29.7.2008	Dne 29.07.2008 byla dodána sestava HSM serveru pro HSM-SKC-Provoz a čtečka pro inicializaci SAM a karet uživatelů SKC (a KAP). Dodávka je součástí akceptačního protokolu č.1 ze dne 14.10.2008.
29.7.2008	Dne 29.07.2008 byla za účasti zástupců HMP, Ing.Ivana Lukeše a Ing.Ivana Seyčka, proběhla v centrálním pracovišti PCKS vzorová ukázka generování klíčů ke kartám MIFARE DESFire. Součástí této ukázky bylo předání přístupových karet k HSM SKC-Provoz a HSM-Záloha příslušným bezpečnostním úředníkům. Protokol o generování klíčů SKC-KAP je součástí akceptačního protokolu č.1 ze dne 14.10.2008 Současně zástupce HMP, Ing.Ivan Lukeš, pověřil zástupce Haguess, Ing.Vladimíra Valdu, aby jej zastupoval při importu klíčů ze systému HSM SKC-Provoz do systému HSM DOS-Root spravovaného DPP. A dále zástupce HMP, Ing.Ivan Seyček, pověřil zástupce Haguess, RNDr.Jana Kodovského, aby jej zastupoval při importu klíčů ze systému HSM SKC-Provoz do systému HSM DOS-Root spravovaného DPP. Oba protokoly o zastupování jsou součástí akceptačního protokolu č.1 ze dne 14.10.2008.
31.7.2008	31.07.2008 Uzavřena smlouva č. INO/40/01/001653/2008 o zpracování osobních údajů ve vztahu ke KAP.
31.7.2008	Dne 31.07.2008 byla uzavřena smlouva č. INO/40/01/001638/2008 o zajištění provozu PCKS na období 1.8.2008 - 31.12.2008. Ve stejný den byl uzavřen dodatek č.1 ke smlouvě o zajištění provozu PCKS č. INO/40/01/001638/2008, který je v podstatě přílohou, obsahující technické parametry.

31.7.2008	31.07.2008 Uzavřena smlouva o dílo č. DIL/40/01/001652/2008 na Rozšíření SKC o technologii MIFARE DESFire.
31.7.2008	31.07.2008 Uzavřena licenční smlouva č. LIC/40/01/001650/2008 na Software SAM pro SKC a KAP. Licence je poskytnuta na SAM-Automat, INI, Prodej, Personalizace.
31.7.2008	31.07.2008 Uzavřena licenční smlouva č. LIC/40/01/001651/2008 na Software ASW HSM-SKC. Licence je poskytnuta na 1 server a inicializaci 1000ks SAM. Smlouva LIC/40/01/001651/2008.

3.5.1. Projektové řízení v období změny karetní technologie

Projektové řízení v období změny karetní technologie bylo pod vedením společnosti Soluziona (dnes Indra). Doslovný přepis.

Datum	Činnost
14.12.2006	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z08, 14.12.2006 Úkol: PCKS-KS-Z06/6 odloženo, Zajistit potvrzení výrobce o termínu dodání karet. (chceme nejzazší termín výroby ?), 7.12., 14.12., 19.12. Zápis o provedených činnostech bod 2.2. Zatím není Chromaline, po jeho obdržení bude potřeba zajistit schválení HGS a MBBDP, předpokládaný termín obdržení Chromaline je do 22.12.
19.12.2006	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z09, 19.12.2006 Zápis o provedených činnostech bod 2.2. Chromaline je na cestě ze Singapuru, předáno PDF, předpokládaný termín obdržení Chromaline je do 22.12., Schvalovat bude BBDO, které zajistí koordinaci schvalování, Bude-li schváleno, očekávaný termín dodávky je okolo poloviny února. Učiněná rozhodnutí: KS rozhodla o vytištění vzorku 200 ks karet jako vzorky v ceně cca 50 000, Kč. (Pozn: 250,-Kč/karta)

4.1.2007	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z10, 4.1.2007 Úkol: PCKS-KS-Z09/1 změněno, Haguess zajistí vytištění 200 ks vzorků karet 31.1.07.
18.1.2007	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z12, 18.1.2007 Zápis o provedených činnostech bod 2.3. Na jednání KS č.02 byla expirace karty schválena na 4 roky. Vzhledem ke zkušební verzi 50 000 Opencard byla navržena doba platnosti 2 roky – vedou k tomu zejména neustále se vyvíjející technologické postupy.
15.2.2007	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z16, 15.2.2007 Zápis o provedených činnostech bod 2.3. Příští týden v pátek budou karty hotovy. Proběhne předávání karet městu.
22.2.2007	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z17, 22.2.2007 Zápis o provedených činnostech bod 2.5. Zatím bylo doručeno 15 000 ks karet. Zbytek bude doručen během března.
15.3.2007	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z20, 15.3.2007 Zápis o provedených činnostech bod 2.10. Všechny karty již dodány. (Následně učiněna změna. Bez odůvodnění, bez informace na jakém základě se učinilo toto rozhodnutí.)
22.3.2007	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z21, 22.3.2007 Zápis o provedených činnostech bod 2.13. Haguess předá karty MHMP a v zápětí předá karty MHMP Haguessu do úschovy. Úkol: PCKS-KS-Z21/1 Provést protokolární předání nových karet Haguess – MHMP – Haguess, 29.3.2007.
29.3.2007	Zápis z jednání týmu KS – koncepční skupina, PCKS-KS-Z22, 29.3.2007

	Úkol: PCKS-KS-Z21/1 splněno, provést protokolární předání nových karet Haguess – MHMP – Haguess, 29.3.2007.

3.5.2. Rok 2009

Datum	Fáze projektu
2.1.2009	Dne 02.01.2009 byla uzavřena smlouva č. INO/40/01/001831/2009 o zajištění provozu PCKS v období 1.1.2009-28.2.2009.
15.1.2009	Dne 15.01.2009 bylo doručeno Oznámení o zrušení zadávacího řízení "Výroba, produktová personalizace a dodávka čipových karet" č.j. INF/40/2009 ze dne 7.1.2009, které bylo zahájeno dne 10.7.2008 odesláním výzvy č.j. INF/849/S-VZ-425323.
31.1.2009	Dne 31.01.2009 byla v souladu se smlouvou č. DIL/40/05/001271/2007 byla vystavena faktura č. FV-3/2009 na servisní podporu informačního systému KAP (v období 1.11.2008-31.1.2009) na částku 146 250 Kč.
4.2.2009	Dne 04.02.2009 byla v souladu se smlouvou č. INO/40/01/001831/2009 ze dne 2.1.2009 o zajištění provozu PCKS vystavena faktura č. FV-5/2009 za období 1.1.2009-31.1.2009 na částku6 627 307 Kč. Současně byla v souladu se smlouvou č. INO/40/01/001831/2009 ze dne 2.1.2009 o zajištění provozu PCKS vystavena faktura č. FV-6/2009 za bezkontaktní karty vydané v období 1.1.2009-31.1.2009 (celkem 33855 ks karet) na částku 5 687 640.
5.2.2009	Dne 05.02.2009 byla doručena Výzva č.j. INF/174/2009 k jednání v jednacím řízení bez uveřejnění na realizaci veřejné zakázky "Zajištění provozu Pražského Centra Kartových Služeb" pro HMP v návaznosti na veřejnou zakázku Realizace SKC. Následně dne 19.02.2009 bylo doručeno oznámení č.j. INF/259/2009 o výběru nejvhodnější nabídky na zakázku Zajištění provozu PCKS po dobu od 1.3.2009 do 30.4.2009 Smlouva č. INO/40/01/001860/2009 o zajištění provozu PCKS v období 1.3.2009 - 30.4.2009 byla uzavřena 26.02.2009.
9.3.2009	Dne 09.03.2009 byla souladu se smlouvou č. INO/40/01/001831/2009 ze dne 2.1.2009 o zajištění provozu PCKS byla vystavena faktura č. FV-11/2009 za bezkontaktní karty vydané v období 1.2.2009-28.2.2009 (celkem 4830 ks karet) na částku 811 440 Kč.

	Současně byla v souladu se smlouvou č. INO/40/01/001831/2009 ze dne 2.1.2009 o zajištění provozu PCKS byla vystavena faktura č. FV-10/2009 za období 1.2.2009-28.2.2009 na částku6 627 307 Kč.
25.3.2009	Dne 25.03.2009 byla doručena výzva č.j. INF/379/2009 k jednání v jednacím řízení bez uveřejnění na zakázku "Zajištění provozu PCKS v období 1.5.2009-31.7.2009".
31.3.2009	Dne 31.03.2009 byla uvedena do provozu kumulativní aktualizace systému SKC a KAP.
6.4.2009	Dne 06.04.2009 byla v souladu se smlouvou č. INO/40/01/001860/2009 ze dne 26.2.2009 o zajištění provozu PCKS vystavena faktura č. FV-14/2009 za období 1.3.2009-31.3.2009 na částku 6 627 307,00
10.4.2009	Dne 10.04.2009 byla v souladu se smlouvou č. INO/40/01/001860/2009 ze dne 26.2.2009 o zajištění provozu PCKS byla vystavena faktura č. FV-16/2009 za bezkontaktní karty vydané v období 1.3.2009-31.3.2009 (celkem 13540 ks karet) na částku 2 274 720,00.
30.4.2009	Dne 30.04.2009 byl uzavřen dodatek č.1 ke smlouvě INO/40/01/001860/2009 o zajištění provozu PCKS po dobu 1.3.2009-30.4.2009 kterým se účinnost smlouvy prodlužuje do 31.5.2009.
5.5.2009	Dne 05.05.2009 byla v souladu se smlouvou č. DIL/40/05/001271/2007 vystavena faktura č. FV-20/2009 na servisní podporu informačního systému KAP (v období 1.2.2009-30.4.2009) na částku 146 250 Kč. Současně byla v souladu se smlouvou č. INO/40/01/001860/2009 ze dne 26.2.2009 o zajištění provozu PCKS vystavena faktura č. FV-19/2009 za období 1.4.2009-30.4.2009 na částku6 627 307 Kč.
7.5.2009	Dne 07.05.2009 byla v souladu se smlouvou č. INO/40/01/001860/2009 ze dne 26.2.2009 o zajištění provozu PCKS byla vystavena faktura č. FV-21/2009 za bezkontaktní karty vydané v období 1.4.2009-30.4.2009 (celkem 10534 ks karet) na částku 1 769 712 Kč.
15.5.2009	Dne 15.05.2009 proběhlo třetí jednání v jednacím řízení bez uveřejnění na zakázku Zajištění provozu PCKS po dobu od 1.5.2009 do 31.7.2009.

25.5.2009	Dne 25.05.2009 bylo doručeno oznámení o výběru nejvhodnější nabídky na zakázku zajištění provozu PCKS v období 1.5.2009 - 31.7.2009. Ve stejný den byla uzavřena smlouva č. INO/40/01/001966/2009 o zajištění provozu PCKS po dobu 1.5.2009-31.7.2009.
2.6.2009	Dne 02.06.2009 byla v souladu se smlouvou č. INO/40/01/001966/2009 ze dne 25.5.2009 o zajištění provozu PCKS byla vystavena faktura č. FV-27/2009 za bezkontaktní karty vydané v období 1.5.2009-30.5.2009 (celkem 2497 ks karet) na částku 419 496 Kč. Současně byla v souladu se smlouvou č. INO/40/01/001966/2009 ze dne 25.5.2009 o zajištění provozu PCKS vystavena faktura č. FV-26/2009 za období 1.5.2009-30.5.2009 na částku 6 627 307 Kč.
30.6.2009	Dne 30.06.2009 byla v souladu se smlouvou č. INO/40/01/001966/2009 ze dne 25.5.2009 o zajištění provozu PCKS vystavena faktura č. FV-31/2009 za období 1.6.2009-30.6.2009 na částku 6 627 307,00 30.06.2009 byla vedena do provozu nová verze systému SKC a KAP obsahující úpravy a nové funkce dle požadavků provozního centra PCKS.

3.6. Nález

V roce 2005 proběhlo předběžné oznámení projektu na centrální adrese. Následná veřejná zakázka však byla v roce 2006 vyhlášena s výrazně vyšší cenou (o 83 milionů). V průběhu posuzování se nepodařilo získat podklady, které by tento rozpor objasnily.

Počáteční nastavení smluvních vztahů v projektu byly z pohledu HMP nevýhodné a společnosti Haguess, jako komerční subjekt, tím získala a využila veškerého vyjednávacího prostoru, které mu smluvní ujednání z roku 2006 a předně způsob řízení projektu objednatelem dovolilo.

Při posuzování licenční politiky jsme dospěli k názoru, že dle smluvní úpravy platné ke 30.6.2009, tedy k datu, ke kterému je zpracováváno toto posouzení, je licence počítána za každou kartu evidovanou v systému, včetně karet, které byly z jakéhokoliv důvodu zrušeny, případně expirovala jejich platnost (původní karty MIFARE Classic mají platnost 2 roky, stávající MIFARE DESFire mají platnost 4 roky). Z tohoto principu plyne teoretický výpočet, že po 4 letech, kdy uplyne platnost stávajících karet, bude nutné zdvojnásobit počet licencí, jelikož v systému budou kromě aktivních karet pro každého uživatele uloženy i informace o jeho předchozí kartě, případně o předchozích kartách! MHP doporučujeme změnit v rámci jednání se společnosti Haguess smluvní podmínky tak, aby byly licenční poplatky účtovány pouze za aktivní karty, využívající alespoň jednu z poskytovaných aplikací. Stávající karty MIFARE DESFire mají ve své datové položce uloženou identifikaci karty, která byla předchůdcem karty vydané, ale způsob evidence lze realizovat i ve formě smluvních reportů a pravidelných vyúčtování.

V průběhu roku 2007 došlo k nastavení smluvních podmínek tak, že bylo proti zavedeným pravidlům a interním metodikám MHMP umožněno proplácet faktury vystavené společností Haguess za provoz kartového centra na počátku měsíce, v němž docházelo k plnění. V praxi sice docházelo na počátku měsíce, v němž docházelo k plnění pouze k vystavení faktury se splatností 30 dní, takže MHMP proplácel částku až po skončení měsíce, ale ani tato praxe není na MHMP obvyklá, jelikož v podstatě docházelo k poskytování zálohy, nebo minimálně k obcházení obvyklé splatnosti faktur. Příkladem může být například faktura č. FV-7/2008 ze dne 4.2.2008, která byla v souladu se smlouvou č. INO/40/01/001386/2007 ze dne 31.10.2007 o zajištění provozu PCKS, vystavena za období 1.2.2008-29.2.2008, tedy na jeho začátku. Tento stav byl v průběhu roku 2008 narovnán a v tuto chvíli je dodržován obvyklý způsob, kdy faktura za daný měsíc je vystavena až cca 10 dní po skončení doby plnění a má splatnost 30 dní, jak je na MHMP obvyklé.

Dne 13.9.2007 proběhl audit v centrálním pracovišti Haguess, provedený společností Relsie s.r.o. na základě objednávky MHMP. Tento audit byl zaměřen hlavně na technologické a bezpečnostní parametry systému. V obecné rovině neshledal žádná fatální pochybení, přesto však uváděl množství doporučení a námětů pro další postup HMP v projektu. V průběhu posouzení se nám podařilo získat informace o tom, že první

kroky vycházející z doporučení Relsie s.r.o. byly ze strany HMP realizovány až v polovině roku 2008. Tato prodleva byla dle informací odboru informatiky způsobena objektivně složitou situací ve vyjednávání změny podmínek se společností Haguess.

Dne 30.06.2008 byla uvedena do provozu nová verze systému SKC a KAP pracující s kartami MIFARE Classic i MIFARE DESFire. Dne 30.06.2008 byla předána nabídka společnosti Haguess na zakázku "Rozšíření SKC o MIFARE DESFire". Z toho plyne, že nová verze systému byla uvedena do provozu současně s podáním nabídky. Při zjišťování příčin tohoto postupu jsme dospěli k závěru, že spuštění nové verze systému SKC a KAP pravděpodobně souviselo s časovým tlakem ze strany dopravních podniků a spuštění dopravní aplikace, která měla podporu MIFARE DESFire ve svých podmínkách. Přesto se nám tuto informaci nepodařilo zcela zřetelně získat z projektové dokumentace.

Dne 29.07.2008 proběhla za účasti zástupců HMP, Ing.Ivana Lukeše a Ing.Ivana Seyčka v centrálním pracovišti PCKS vzorová ukázka generování klíčů ke kartám MIFARE DESFire. Součástí této ukázky bylo předání přístupových karet k HSM SKC-Provoz a HSM-Záloha příslušným bezpečnostním úředníkům. Protokol o generování klíčů SKC-KAP je součástí akceptačního protokolu č.1 ze dne 14.10.2008.

Jako porušení bezpečnostních pravidel a současně obcházení svých povinností jsme vyhodnotili situaci, kdy ve stejný den zástupce HMP, Ing.Ivan Lukeš, pověřil zástupce Haguess, Ing. Vladimíra Valdu, aby jej zastupoval při importu klíčů ze systému HSM SKC-Provoz do systému HSM DOS-Root spravovaného DPP. A dále zástupce HMP, Ing.Ivan Seyček, pověřil zástupce Haguess, RNDr.Jana Kodovského, aby jej zastupoval při importu klíčů ze systému HSM SKC-Provoz do systému HSM DOS-Root spravovaného DPP. Zodpovědní pracovníci MHMP se tímto vzdávají jedné z možností kontrol, případně možnosti podílet se na projektu. Tento stav narovnán až v průběhu roku 2008 a od tohoto okamžiku jsou „klíče" v rukách zodpovědných pracovníků MHMP.

Projektové řízení v období změny karetní technologie bylo pod vedením společnosti Soluziona (dnes Indra). Doporučení původní technologie MIFIRE Classic pro pilotní provoz a jeho následné nahrazení technologií MIFIRE DESFire je v souladu s původní předprojektovou studií společnosti Soluziona „Pražské centrum kartových služeb" datovanou do roku 2005. Z tohoto pohledu konstatujeme, že problém změny karetní technologie přisuzujeme špatnému projektovému rozhodnutí v době realizace projektu (2007), kdy se podmínky nasazování jednotlivých typů karet od původní studie změnily. Volba karty MIFIRE Classic pro pilotní projekt, namísto v době již běžně využívané karty MIFARE DESFire pak v konečném důsledku znamenala zbytečně vynaložené náklady na pořízení více jak 45 050 karet, které nebyly nikdy využity, a současně vedla k placeným úpravám celého systému. Rozdíl ceny obou karet v daném čase není při zvoleném počtu karet dostatečně významný, aby vynaložené náklady na změnu systému vyvážil. I přes toto špatné rozhodnutí se však dalo minimálně části zbytečně vynaložených nákladů zabránit tím, že by byl nakoupen pro pilotní provoz menší počet karet

standardu MIFIRE Classic, případně by byly dle původních předpokladů dodrženy i propagační a marketingové aktivity, které předpokládaly vyšší rozšíření karet mezi uživatele již v pilotním provozu.

3.7. Normy, technologie, bezpečnost, dokumentace a legislativní rámec karty. Použité vstupy a informační zdroje

Níže uvedený seznam norem obsahuje normy, které jsou důležité pro danou problematiku a měly by být dodržovány. Z důvodu rozsahu a časového rámce projektu nebylo možné provést detailní kontrolu dodržování všech uvedených norem.

Karty

- ČSN ISO/IEC 7816 – Identifikační karty - Karty s integrovanými obvody s kontakty
- ČSN ISO/IEC 7810 – Identifikační karty - Fyzikální charakteristiky
- ČSN ISO/IEC 14443 – Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s vazbou na blízko
- ČSN ISO/IEC 7812 – Identifikační karty - Identifikace vydavatelů karet
- ČSN ISO/IEC 10373 – Identifikační karty - Zkušební metody

ČSN ISO/IEC 10202 – Identifikační karty - Karty pro finanční transakce – Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody

Zabezpečení dat na kartě

- AN155010 – End to end system security risk considerations for implementing contactless cards (NXP, June 2008)
- AN155121 – End to end system security risk considerations for implementing MIFARE Classic (NXP, February 2009)
- AN10787 – MIFARE Application Directory (MAD), NXP, March 2009
- MF3ICD21, MF3ICD41, MF3ICD81 – MIFARE DESFire EV1 contactless multi-application IC, NXP, March 2009 Product short data sheet

Formát dat na kartě

- ČSN EN 1545 - Systémy identifikačních karet - Aplikace pro povrchovou dopravu - Datové prvky a seznam kódů pro související dopravní a cestovní platby
- Vyhláška č. 175/2000 Sb., o přepravním řádu pro veřejnou drážní a silniční osobní dopravu – požadavky na jízdní doklad

Správa kryptografických klíčů

- ČSN ISO/IEC 11770 – Informační technologie – Bezpečnostní techniky – Správa klíčů

Bezpečnost politika, dokumentace a opatření

Při zpracování Bezpečnostní politiky, Bezpečnostní dokumentace jakož i při realizaci konkrétních bezpečnostních opatření, je čerpáno z následujících norem:

- ČSN ISO/IEC 17799 – Informační technologie – Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací (POZN. Dnes norma ČSN ISO/IEC 27001)
- ČSN ISO/IEC TR 13335 – Informační technologie - Směrnice pro řízení bezpečnosti IT

Vývoj, implementace a servis aplikačního software

Při řízení vývoje, jeho implementace a rozvoje bylo využito vedle vnitrofiremních procesů HGS doporučení uvedená v normě:

- ČSN ISO/IEC 12207 - Informační technologie - Procesy v životním cyklu software
- .NET Framework (vlastník Microsoft) - ISO/IEC 23271:2006 and ISO/IEC 23270:2006, Ecma - Ecma International)
- Microsoft Windows prostředí (Team Foundation Server)
- ISO/IEC 9075:1992 - Database Language SQL (SQL-92)
- Oracle SQL
- „Open Platform" : OS, freeware

SAM moduly

- Java Card 2.1.1
- FIPS 140-2 – „Security Requirements for Cryptographic Modules"
- IEEE P1363

HSM (Protect Server Gold 220, Safenet)

- PKCS#11
- Certifikace kryptokarty dle Safenet:
  - FCC Part 15 - Class B
  - RoHS-compliant
  - BAC and EAC ePassport certification
  - ProtectServer Gold: FIPS 140-2 Level 3 Certificate #739 & #1137
  - ProtectServer Internal-Express: FIPS validation in progress
  - FCC Part 15 Class B Unintentional Radiators ANSI C63.4-2003
  - EN 55022:1998 Amendment 1:2000, Amendment 2:2003
  - EN 55024:1998 Amendment 1:2001

Web Service

- W3C: RFC 4743 WSDL
- W3C: RFC 2616 (rfc2616) - Hypertext Transfer Protocol
- RFC 2459: Internet X.509 Public Key Infrastructure

Sítě

- RFC
- W3C
- GSM

Zajištění provozu PCKS

- zákon č. 101/2000 Sb., o ochraně osobních údajů – osobní údaje jsou informační aktiva, jejichž ochraně je ve všech provozovaných produktech i při výkonu procesních operací mimo ně, věnována maximální pozornost. Uspořádání produktů celého řešení PCKS umožňuje plně aplikovat požadavky tohoto zákona.
- zákon č. 513/1991 Sb., obchodní zákoník - definice obchodního tajemství, označení důvěrných informací, bezpečnostní požadavky ve smlouvách
- zákon č. 65/1965 Sb., zákoník práce - personální bezpečnost, zaměstnanec jako uživatel, vzdělávání, kontrola, odpovědnost za škodu
- zákon č. 121/2000 Sb., autorský zákon – přesné licenční smlouvy, z toho plynoucí práva a povinnosti v pracovním řádu a pracovní smlouvě, pravidla ochrany softwaru, kontroly licencí.
- zákon č. 563/1991 Sb., o účetnictví
- zákon č. 97/1974 Sb., o archivnictví – při vedení spisovny se řídíme některými ustanoveními tohoto zákona ve spisovém a skartačním řádu
- zákon č. 124/2002 Sb., o platebním styku – vymezení elektronických peněz a elektronických peněžních prostředků.

Dokumentace

- vyhláška č.529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy – přihlídnuto k požadavkům na strukturu provozní dokumentace.

3.8. Použité vstupy a informační zdroje

3.8.1. Realizace SKC 2006

- Zadávací dokumentace
- Realizace SKC -svazek č.1, kvalifikace 21.8.2006
- Realizace SKC -svazek č.2, nabídky 25.8.2006
  - Rozhodnutí o přidělení zakázky 29.9.2006
- Smlouva o dílo DIL/40/05/001120/2006 23.10.2006
  - Realizace
  - Podpora po dobu 4 let
- Licenční smlouva LIC/40/05/001128/2006 6.11.2006
- Servisní smlouva INO/40/05/001127/2006 6.11.2006

3.8.2. Realizace SKC 2006 - 2007

- Pravidla pro řízení kvality, metodika řízení projektu – vypracovala fy. Soluziona
  - Řízení kvality,
  - Projektový plán – plánované kontroly
  - Měřítko dodržení metodické jednotnosti jednotlivých projektů
- Pravidla pro řízení rizik projektu PCKS
  - Registr rizik udržovaný v elektronické podobě
- Pravidla pro vedení projektové dokumentace
- Podmínky realizace projektu SKC – harmonogram realizace

- MHMP požaduje další provoz a rozvoj SKC externím subjektem po dobu 5 let 2.5.2007
- Vyhodnocení pilotního provozu PCKS (SKC) 12.4.2007
  - Zpožděná realizace „bezpečný přístup na portál"
- Podpis akceptačního protokolu 30.9.2007
- Realizace SKC
  - Specifikace řešení Městské knihovny 8.12.2006
  - Bezhotovostní úhrady pakování 15.12.2006
  - Přístup na portál MHMP 15.12.2006

3.8.3. HMP KAP-1 2007 – výzva, nabídka, oznámení, smlouvy, předávací protokoly, faktury

- Výzva k jednání v jednacím řízení bez uveřejnění, INF 213/2007, vyřizuje Ing. Chytil, 1.2.2007
  - Předmět realizace „Kartové aplikace parkování" – licence KAP pro min. 50 tis. Držitelů ČK a provoz min na 150 parkovacích automatech, dodávka systémového vybavení, zajištění úpravy stávajících parkovacích aut. v počtu 143, návrh procesů a vazeb na „Servisní kartové centrum" a MHMP, zajištění zkušebního provozu na 6 měsíců, podpora a údržba po dobu 2 let
  - Doba plnění do 31.12.2009
- Protokol o jednání k výzvě 8.2.2007, přítomni za zadavatele: Ing. Jiří Chytil (vedoucí odd. INF MHMP), Ing. Zdeněk Pliška (referent spec. DOP MHMP), Vladimír Kašpar (odborný konzultant), Ing. Jan Marek , (referent spec. DOP MHMP); za uchazeče: Ing. Jiří Bláha; tajemnice komise: JUDr. Ludmila Krejčová (odbor INF MHMP)
  - Cena licence 50 tis. + 150 1.613.500,- bez DPH, HW a SW 401.515,-, úprava stávajících parkomatů 6.359.980,-, dvouletý servis KAP 1.170.000,-, zkušební provoz 6 měsíců 505.100,-
  - Akceptace formou předávky a předvedení funkčního řešení
- Nabídka realizace KAP 6.2.2007
  - Smlouva o dílo,
  - Specifikace systémového HW a SW
  - Specifikace úprav park. Automatů
  - Vzor- smlouva o poskytnutí služeb servisu KAP
  - Podrobný časový harmonogram
  - Popis kartové aplikace včetně licenčních podmínek
- Smlouva o dílo INO/40/05/001270/2007 26.2.2007
- Smlouva o poskytnutí služeb servisu KAP DIL/40/05/001271/2007 26.2.2007
- Licenční smlouva LIC/40/05/001272/2007 26.2.2007
- Předávací protokoly
  - Licence KAP 5.3.2007
  - Soubor upravených parkovacích automatů 12.4.2007, 26.4.2007, 30.4.2007, 10.5.2007, 18.5.2007
  - HW a SW 18.5.2007

3.8.4. Podklady pro rozvoj KAP – objednávka, potvrzení objednávky, výsledné dokumenty, předávací protokoly, faktura

KAP II 2008 - výzva, nabídka, oznámení, smlouvy, předávací protokoly, faktury

HMP Provoz PCKS od 1.4.2007 do 31.10.2007 – výzva, nabídka, oznámení, smlouvy, faktury

- Nabídka 15.3.2007
- Oznámení o výběru INF 597/2007 27.3.2007
- Smlouva INO/40/05/001296/2007 12.4.2007
- Dodatek ke smlouvě č. 1 INO/40/05/001296/2007 24.9.2007
- Dodatek ke smlouvě č. 2 INO/40/05/001296/2007 26.9.2007
- Smlouva „o vydání a správě karet OC" MAN/40/05/001297/2007 12.4.2007
- Dodatek ke smlouvě „o vydání a správě karet OC" č. 1 MAN/40/05/001297/2007 24.9.2007
- Smlouva „o zpracování osobních údajů" INO/40/05/001298/2007 12.4.2007
- Dodatek ke smlouvě „o zpracování osobních údajů" INO/40/05/001298/2007 24.9.2007
- Faktury – vždy za dané časové období provozu

3.8.5. HMP Provoz PCKS od 1.11.2007 do 31.7.2008 – výzva, nabídka, oznámení, smlouvy, faktury

- Výzva k jednání v jednacím řízení bez uveřejnění INF 1701/2007 11.10.2007
- Nabídka „Provoz PCKS" 15.10.2007
- Oznámení o výběru INF 1713/2007 16.10.2007
- Smlouva o zajištění provozu PCKS INO/40/01/001386/2007 31.10.2007
- Smlouva o vydání a správě karet OC MAN/40/01/001387/2007 31.10.2007
- Smlouva o zpracování osobních údajů INO/40/01/001388/2007 31.10.2007
- Dodatek č. 1 k INO/40/01/001388/2007 31.10.2007
- Fakturováno po měsíční periodě

3.8.6. HMP Provoz PCKS od 1.8.2008 do 31.12.2008 – výzva, nabídka, oznámení, smlouvy, faktury

- Výzva k jednání v jednacím řízení bez uveřejnění INF 805/2008 4.7.2008
- Nabídka „provoz PCKS" 14.7.2008
- Smlouva o zajištění provozu SKCP INO/40/01/001638/2008 31.7.2008
- Dodatek č. 1 o zajištění provozu SKCP INO/40/01/001638/2008 31.7.2008
- Smlouva o zpracování osobních údajů INO/40/01/001653/2008 31.7.2008
- Měsíční fakturace

3.8.7. HMP Provoz PCKS od 1.1.2009 do 28.2.2009 – výzva, nabídka, oznámení, smlouvy, faktury

- Výzva k jednání v jednacím řízení bez uveřejnění INF 1636/2008 20.11.2008
- Nabídka „provoz PCKS" 19.12.2009
- Smlouva o zajištění provozu SKCP INO/40/01/001831/2008
- Smlouva o zpracování osobních údajů INO/40/01/001653/2008 31.7.2008
- Měsíční fakturace

3.8.8. Použité vstupy a informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společnosti Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace s DPP
- Projektová dokumentace Soluziona
- Konzultace Deloitte
- Metodiky projektového řízení – Best Practices

4. Rekapitulace projektu mezi DPP a Haguess

DPP se dlouho stavěl k projektu Opencard neutrálně a o zapojení do projektu neměl zájem. DPP chtěl jít vlastní cestou a to že on sám by byl emitentem. Ve světě jde o obvyklé řešení, jelikož dopravní podniky disponují kritickým kmenem uživatelů pro podobné aplikace. Vlastní zapojení do projektu proběhlo až v druhé polovině roku 2007.

4.1.1. Rok 2007

Datum	Fáze projektu
22.8.2007	Dne 22.08.2007 byla uzavřena smlouva č. NDA-072208 o mlčenlivosti a utajení informací. Účelem na něž se smlouva vztahuje, je projekt Dopravně - odbavovacího systému Dopravního podniku. Smlouva platí 5 let od data jejího uzavření.
15.10.2007	Poté byla dne 15.10.2007 zavřena smlouva o dílo č. DIL-071510 na Software DOS a současně licenční smlouva č. LIC-071510 na Software DOS pro 50.000 evidovaných uživatelů s aktivovanou kartovou aplikací DOS, 250 POS a 25 PC. Termín dodávky licence byl do 7.12.2007.
7.12.2007	Dne 07.12.2007 předal v souladu se smlouvou o dílo DIL-071510 a licenční smlouvou č. LIC-071510 ze dne 15.10.2007 zástupce Haguess zástupci DPP licenci software typu B.IV.2. Současně v souladu se smlouvou o dílo DIL-071510 a licenční smlouvou č. LIC-071510 ze dne 15.10.2007 a jejím článkem 5 byla vystavena faktura č. FV-44/2007 na poplatek za licenci software typu B.IV.2 ve výši 11 052 500 CZK.

4.1.2. Rok 2008

Datum	Fáze projektu
15.5.2008	Dne 15.05.2008 byla předána nabídka na "Dopravní odbavovací systém - Dodávka software". Nabídkou je návrh smlouvy o dílo. 15.05.2008 proběhlo otevírání obálek s nabídkami účastníků v jednacím řízení bez uveřejnění na zakázku "Dopravní odbavovací systém - Dodávka Software" a ihned proběhlo první jednání v jednacím řízení bez uveřejnění na zakázku "Dopravní odbavovací systém - Dodávka Software". Cílem jednání byla konkretizace předmětu plnění. Druhé jednaní v jednacím řízení bez uveřejnění na zakázku "Dopravní odbavovací systém - Dodávka Software" proběhlo 30.05.2008. Cílem bylo jednání o nabídkové ceně.
19.6.2008	Dne 19.06.2008 byly u končeny akceptační testy DOS - Prodejní místo provedené formou kontroly software proti testovacím scénářům. Testovací scénáře jsou odsouhlaseny osobou oprávněnou za DPP a osobou oprávněnou za Haguess.
27.6.2008	Dne 27.06.2008 byly ukončeny akceptační testy DOS - Administrace systému provedené formou kontroly software proti testovacím scénářům. Testovací scénáře jsou odsouhlaseny osobou oprávněnou za DPP a osobou oprávněnou za Haguess. Ve stejný den byly ukončeny akceptační testy DOS - SAM moduly a odemykací karty provedené formou kontroly software proti testovacím scénářům. Testovací scénáře jsou odsouhlaseny osobou oprávněnou za DPP a osobou oprávněnou za Haguess.
30.6.2008	Dne 30.06.2008 bylo přijato rozhodnutí zadavatele o výběru nejvhodnější nabídky na zakázku "Dopravní odbavovací systém - Dodávka Software".
3.7.2008	Dne 03.07.2008 předal zástupce Haguess zástupci DPP 750 ks karet MIFARE Classic (odebráno ze skladové zásoby karet MHMP) pro účely ověřovacího provozu DOS. Karty byly personalizovány dle údajů zaměstnanců předaných zástupcem DPP.
15.7.2008	Dne 15.07.2008 byla uzavřena smlouva o dílo za dodávku licencí DOS, SAM, ASW-HSM-DOS a následující den byly provedeny integrační testy DOS - SAP R3a kontrolní zátěžový test uzávěrky DOS a přenosu relevantních informací do SAP R3. Součástí testu byla i

	kontrola správnosti výpočtu ceny kuponů (časové rozlišení) a funkcionality DOS-SAP R3
18.7.2008	Dne 18.07.2008 převzal zástupce DPP certifikáty opravňující DPP k užívání software DOS, SAM, ASW-HSM-DOS.
10.12.2008	Dne 10.12.2008 byla doručena výzva k účasti v jednacím řízení bez uveřejnění na zakázku rozšíření licence DOS. Současně byla doručena zadávací dokumentace na rozšíření licence systému DOS v rámci jednacího řízení bez uveřejnění na licenci umožňující vedení informací pro 350.000 evidovaných uživatelů s nahranou kartovou aplikací DOS.
12.12.2008	Dne 12.12.2008 proběhlo první jednání v jednacím řízení bez uveřejnění na zakázku rozšíření licence DOS. V rámci jednání bylo dohodnuto bezúplatné užívání poskytnuté licence po dobu 6 měsíců od data účinnosti dodatku smlouvy.
15.12.2008	Dne 15.12.2008 byl uzavřen dodatek č.1 ke smlouvě o dílo ze dne 15.7.2008 na rozšíření licence DOS na úroveň vedení informací pro 350.000 evidovaných uživatelů s nahranou kartovou aplikací DOS a současně byla formálně uzavřena dodávka funkcí DOS v rozsahu: Reporty prodaných kuponů, Výstupní protokoly z Kontrolního modulu. Dále bylo formálně uzavřeno odstranění následujících výhrad DPP k aplikaci DOS: Oprava způsobu evidence duplikátů (žádost o opravu funkcionality DOS, ze dne 6.11.2008), Automatizovaný import dat z SKC (žádost o opravu funkcionality DOS, ze dne 6.11.2008), Oprava ASW DOS při stanovení ceny kuponů pro uzávěrku (předáno hlášení problému z HelpDesk DPP, dne 1.12.2008). Ve stejný den bylo formálně uzavřeno odstranění následujících výhrad DPP: automatický přesun nepřenesených kuponů z důvodu chyby síťového připojení při odesílání kuponu. (Žádost o doplnění funkcionality DOS ze dne 13.10.2008).
16.12.2008	Dne 16.12.2008 byla doručena výzva k účasti v jednacím řízení bez uveřejnění na zakázku rozšíření funkcionality DOS a současně s ní i zadávací dokumentace na rozšíření funkcionality systému DOS v rámci jednacího řízení bez uveřejnění.

18.12.2008	Dne 18.12.2008 proběhlo první jednání v jednacím řízení bez uveřejnění na zakázku rozšíření funkcionality DOS.
22.12.2008	Dne 22.12.2008 byl zavřen dodatek č.2 ke smlouvě o dílo ze dne 15.7.2008 na rozšíření funkcionality DOS.

4.1.3. Nevyřešené požadavky DOS

I přesto, že systém je provozován, vykazoval DPP k 30.6.2009 množství výhrad, které DOS považuje za nevyřešené. (Část z těchto výhrad byla vyřešena ve druhém pololetí 2009.) Dále viz.tabulka níže, zápisy z help desku.

Číslo HD	Požadavek
9	V současném stavu při vytvoření duplikátu (dělá externí firma) není zaznamenán údaj o pracovišti, na kterém byl vyroben (SAM) a uživatel. Stejně je zavádějící informace ve sloupci card_kontakt_id (všechny objednávky duplikátů jsou z internetu). Při duplikátu z duplikátu hlásí nulovou cenu v doplatkové pokladně. Požadovaný stav: doplnit tyto informace do DB z důvodu bezpečnosti prodeje duplikátů. Upravit cenu duplikátu pro případ kontroly.
10	V současném stavu jsou Vratky evidovány (účetně) pouze na jednoho uživatele a prodejní organizaci. Požadovaná změna: možnost rozlišit uživatele a organizaci pro kontrolu vrácených peněz a zároveň upravit rozhraní DOS SAP.
14	Při zadávání zařízení (např.:validátory), není možná oprava ani mazání záznamu.
15	Částečně vyřešeno, vráceno – V aplikaci backoffice není možno řadit jakýkoliv výstup. Např. při vyjetí seznamu uživatelů, není možno data (stovky záznamů) nijak filtrovat/srovnat/vyhledat.
17	U dodaných kontrolních modulů „Prodejní místa" a „Validátory" je naprosto nejasná jejich funkce a jejich využití je naprosto nulové, respektive výstupy z nich nepoužitelné. (Bude potřeba odd. OC o této funkcionalitě blíže informovat, případně dodat nějaký help/návodku.
18	Nebyl doposud dodán kontrolní modul (prováděcí projekt 4.1.1.1.3.4)
19	Nebyl dodán modul pro nouzovou synchronizaci (prováděcí

	projekt 4.1.1.1.6.6)
21	V reportním modulu nejsou některé sestavy (prováděcí projekt 4.1.1.5.2) doplnit prodej kupónu na jednotlivých prodejních místech, statistiky podle jednotlivých kategorií a pásmech, sumární přehledy podle počtu pásem i podle kombinací jednotlivých pásem, protokoly o odpuštěných pokutách, přehled duplikátů, výstupní protokoly z kontrolního modulu.
22	Zamítnuto – Neexistuje popis databáze, popis vazeb mezi tabulkami, včetně popisků tabulek - vlastníkem licence je Haguess a.s. nikoliv DP Hl. Města Prahy. Ten je pouze smluvním uživatelem licence. Popis databáze, vazeb mezi tabulkami a popis tabulek je duševním vlastnictvím poskytovatele licence.
23	Zamítnuto – Neexistuje popis funkcionality celého systému, včetně jednotlivých vazeb mezi jednotlivými složkami systému – včetně konkrétních názvů serverů, web služeb apod. Popis systému lze rozdělit na několik částí: 1. HW popis (servery, routery, huby, kabeláž, PC, tiskárny, monitory, apod.) 2. ASW popis (moduly, softwarové knihovny, apod.) Add 1) popis HW existuje v Prováděcím projektu DOS, příloha č.4 Přehled datových toků ze dne 13.2.2008. Je v odpovědnosti vlastníka licence, aby si provedl pro potřeby provozování aktualizaci tohoto popisu pro potřeby provozování nebo aby zadal tuto činnost dodavatelské firmě. (Společnost Haguess a.s., Servisní centrum je připraveno předat nabídku na tuto činnost do 3 týdnů od oficiálního vyžádání) Add 2) Popis ASW je uveden v uživatelských příručkách.
28	Analyzovat příčiny problémů a navrhnout systémové řešení pro odstranění problémů s výpadky serveru a HSM. Identifikovat, jestli existuje řešení nastavení prostředí. Pokud ne, dodat návrh opatření (případně kontaktovat Oracle specialisty) jako podklad pro rozhodnutí IT DPP o dalším postupu.
30	Zamítnuto – Vytvořit přístupové role pro prodej testovacích kupónů – nedoporučuje se vytvářet role pro prodej testovacích kupónů/karet. DOPORUČUJE SE: Zřídit celé jedno DOS pracoviště se všemi potřebnými periferiemi, PC a software, které bude umožňovat prodej kupónů (karty s ostrými klíči, ale potisk karet bude jiný než potisk běžně

	prodávaných karet) – je to lepší návrh řešení, než je uveden v RFS00031.
32	V jednání – Analýza procesů duplikátů karet s doporučeným opatření. Ze strany společnosti Haguess a.s. bude poskytnuta na vyžádání součinnost pro aktivitu analýza procesů duplikátů karet, kterou měl provést zpracovatel (společnost Deloitte and Touche) formou dodatku k již existujícím procesů. Společnost Haguess a.s. je připravena předat do 4 týdnů od vyžádání nabídku na provedení analýzy duplikátu karet místo původního zpracovatele a je zároveň připravena předat nabídku případným softwarovým úpravám vyplývajících z analýzy.
33	Vyjádření k prokazatelnější identifikaci cestujících s nárokem na sníženou přirážku k jízdnému.
39	Nefunkční uzávěrka BW.
45	Dochází k situacím, kdy neproběhne korektně přenos zaplacených kupónů do DOS. DOS dostane informaci, že je kupón zaplacen, ale potvrzení o přijetí této informace nedorazí zpátky do eShopu. V rámci opravy pak eShop opakovaně (každých 15 minut) posílá tuto informaci do DOSa DOS odpovídá chybou, kvůli neočekávanému stavu. Existují dvě možnosti řešení: DOS přijme i duplicitní zprávu o zaplacení kupónu a odpoví OK, čímž dojde k nápravě automaticky. Bude vydefinován podrobný přehled chybových kódů, které DOS vrací tak, aby eShop mohl rozpoznat konkrétní chybový stav (v tomto případě, že kupón již byl zaplacen) a zajistit nápravu u sebe.
46	Je vyžadována součinnost s Haguess v rámci testování nové zprávy OBJEDNÁVKA (přenos párovacích informací mezi objednávkou v eShopu a kupóny v DOS).
47	Bylo by vhodné dohodnout i chybové kódy z DOS pro všechny fáze nákupu tak, any GUI eShopu mohlo adekvátně reagovat a uživatel tak byl odstíněn od jakýkoliv viditelných pádů aplikace.
50	Každý den dochází minimálně ke dvěma závadám validátorů. Validátor je nastartovaný má úvodní obrazovku, ale po vložení karty se nic neděje. V asi 30% za posledních 21 dní není možný vzdálený přístup a validátor se musí restartovat na místě.
54	Na sestavě vratek v DOS nesouhlasí celkový součet poplatků.

55	Žádám dodání dokumentace k databázovému serveru, která by umožňovala správu tohoto serveru. Požadovaný obsah dokumentace je uveden v příloze.
	Zprovoznění testovacího prostředí s tím, aby bylo možno používat ostrá data (prodejní místo, validátor, e-shop, HSM)
	Dořešit problém zálohování aplikačního serveru – na základě dohody o ukončení testování fy. Haguess.
	Provedení testu zprovoznění aplikace DOS v záložní lokalitě.
	Aktivace zaznamenávání úspěšných a neúspěšných událostí o přihlášení – zajištění pravidelného vyhodnocování osobou, která není administrátorem systému (určený pracovník JIT).

4.1.4. Zátěžové testování systému a změnová řízení

Datum	Fáze projektu
21.7.2008	Dne 21.07.2008 byl proveden kontrolní zátěžový test tisku pokladních dokladů na prodejním místě DPP. Celkem bylo prodáno 533 kuponů paralelně na 6 pracovištích. Byla tak otestována konfigurace pracoviště, která bude nasazena na prodejní místa DPP.
22.7.2008	Dne 22.07.2008 byla v souladu se smlouvou o dílo ze dne 15.7.2008 vystavena faktura č. FV-32/2008 za licence DOS, software SAM a ASW HSM-DOS na částku 45 520 000 Kč.
23.7.2008	Dne 23.07.2008 předal zástupce společnosti Haguess zástupci DPP 10 ks karet MIFARE Classic (odebráno ze skladové zásoby karet MHMP) pro účely ověřovacího provozu DOS. Karty byly personalizovány dle údajů zaměstnanců předaných zástupcem DPP.
25.7.2008	Dne 25.07.2008 byla přijata žádost o změnu funkcionality DOS č.3 - Rozšířit obrazovku načtení karty o informaci zda na kartě je datum narození (nikoli zobrazení data narození) a dále žádost o změnu funkcionality DOS č.2 - Předělat výběr pásem na jedno kliknutí myší.
29.7.2008	Dne 29.07.2008 proběhla ceremonie generování kryptografických klíčů DOS. Součástí ceremonie bylo předání přístupových karet a kódů k HSM pověřeným osobám DPP a provedení importu relevantních klíčů SKC do HSM DOS.
31.7.2008	Dne 31.07.2008 byla přijata žádost o změnu funkcionality DOS č.1 - Aplikace DOS - modul inicializační linka SAM nebude SAM zamykat po provedené inicializaci odemykací karty.
7.8.2008	Dne 07.08.2008 provedl zástupce společnosti Haguess jakožto výrobce SAM modulů import klíčů do HSM DOS-Root za účelem inicializace SAM modulů DOS určených pro dopravce PID.
8.8.2008	Dne 08.08.2008 byla přijata objednávka od DPP č. 9016003431 na licence systému DOS, Software SAM, ASW-HSM-DOS na základě smlouvy o dílo ze dne 15.7.2008.

16.8.2008	Dne 16.08.2008 byla přijata žádost DPP o změnu funkcionality HSM - dodat další kartu pro auditora, ukládat logování operací na HSM do externí databáze.
19.8.2008	Dne 19.08.2008 odsouhlasil zástupce DPP návrh řešení změny funkcionality ASW HSM předložený zástupcem Haguess na základě žádosti DPP ze dne 16.8.2008.
19.8.2008	Dne 19.08.2008 provedl zástupce Haguess jakožto výrobce SAM modulů import transportního klíče do HSM DOS za účelem provedení integračních testů DOS a čtečky revizora.
25.8.2008	Dne 25.08.2008 byla ukončena akceptace DOS s výhradami. Přílohou akceptačního protokolu jsou testovací scénáře pro jednotlivé části DOS, testované zástupci DPP a dodavatele (Haguess).
5.9.2008	Dne 05.09.2008 byla přijata žádost o změnu funkcionality DOS č.4 - Poskytnutí slevy na roční kupon pro držitele Opencard, kteří o kartu požádali do 20.9.2008.
10.9.2008	Dne 10.09.2008 předal zástupce společnosti Haguess předal zástupci DPP soubor technické a uživatelské dokumentace k aplikaci DOS v elektronické a písemné podobě.
18.9.2008	Dne 18.09.2008 byla ukončena akceptace komunikační vazby aplikace DOS a čtečky přepravního kontrolora. Akceptační testy proběhly 17-18.9.2008 dle scénářů, které jsou součástí akceptačního protokolu. Současně odsouhlasil zástupce DPP návrh řešení změny funkcionality DOS předložený zástupcem Haguess na základě žádosti DPP č.4 ze dne 5.9.2008.
23.9.2008	Dne 23.09.2008 bylo formálně uzavřeno odstranění výhrad DPP k aplikaci DOS, které DPP vznesl při testování aplikace 27.6.2008. Zástupce společnosti Haguess předal zástupci DPP soubor technické dokumentace k aplikaci DOS v elektronické a písemné podobě. Byla ukončena akceptace úpravy ASW HSM-DOS provedené na základě žádosti o změnu funkcionality HSM ze dne 16.8.2008 a návrhu řešení odsouhlaseného stranou DPP dne 19.8.2008. Proběhla ceremonie předání čtecích kryptografických klíčů aplikace DOS do HSM Českých drah.

24.9.2008	Dne 24.09.2008 bylo formálně ukončeno odstranění výhrad DPP k aplikaci DOS vznesených při akceptačních testech dne 16.6.2008.
29.9.2008	29.09.2008 předal zástupce DPP zástupci Haguess celkem 8 ks odemykacích karet pro obsluhu přepážek kontaktních míst PCKS. Jedná se o karty k pracovišti DOS, které umožňuje nahrát duplikát kuponu.
1.10.2008	Dne 01.10.2008 byla ukončena akceptace úpravy aplikace DOS dodané společností Haguess v souladu s žádostí o změnu funkcionality DOS č.3 přijaté od DPP dne 25.7.2008, dále akceptace úpravy aplikace DOS dodané společností Haguess v souladu s žádostí o změnu funkcionality DOS č.4 přijaté od DPP dne 5.9.2008 a současně akceptace úpravy aplikace DOS dodané společností Haguess v souladu s žádostí o změnu funkcionality DOS č.2 přijaté od DPP dne 25.7.2008, upravit výběr pásem na jedno kliknutí myší. Také bylo formálně ukončeno odstranění výhrad DPP k aplikaci DOS - modul inicializační linka vznesených při akceptačních testech dne 27.6.2008.
8.10.2008	Dne 08.10.2008 byla v souladu se smlouvou o poskytování služeb ze dne 15.9.2008 vystavena faktura č. FV-61/2008 za konzultační služby související s provozem zařízení USV v návaznosti na Opencard/DOS na částku 2 385 896 Kč.
9.10.2008	Dne 09.10.2008 byla přijata žádost DPP o opravu funkcionality DOS: opravit výpočet vratky dle platného ceníku pro daný kupon.
13.10.2008	Dále 13.10.2008 byla přijata žádost DPP o doplnění funkcionality DOS: doplnit do modulu vratky tiskové výstupy za den, měsíc a období. Současně byla přijata žádost DPP o doplnění funkcionality DOS: automatický přesun nepřenesených kuponů z důvodu chyby síťového připojení při odesílání kuponu.
20.10.2008	Dne 20.10.2008 byla uzavřena smlouva č. DIL/40/01/001684/2008 o umožnění provozování kartové aplikace s využitím karty Opencard mezi HMP, jakožto garantem a vydavatelem karty, a DPP, jakožto provozovatelem kartové aplikace DOS. Garant umožňuje provozovateli přístup k PCKS a využít možnosti karty Opencard.

22.10.2008	Dne 22.10.2008 předal zástupce DPP zástupci společnosti Haguess celkem 2 pracoviště DOS, která umožňují nahrát duplikát kuponu.
30.10.2008	Dne 30.10.2008 byly podpisem akceptačního protokolu formálně ukončeny akceptační testy Aplikace DOS - modul pro doplatkovou pokladnu a pracoviště stížností a reklamací. Zástupci DPP provedli za účasti zástupců společnosti Haguess test prodeje kuponů na anonymní kartu na testovacím prostředí DOS. Také bylo formálně uzavřeno odstranění následujících výhrad DPP k aplikaci DOS: Opravit výpočet vratky dle platného ceníku pro daný kupon (Žádost o opravu funkcionality DOS, ze dne 9.10.2008), Doplnit vratky o tiskové výstupy za den, období a měsíc (Žádost o doplnění funkcionality DOS, ze dne 13.10.2008).
30.10.2008	Ve stejný den byla ukončena formálně akceptace úpravy aplikace DOS dodaná společností Haguess na základě žádosti o změnu funkcionality DOS vznesené DPP dne 16.9.2008 - Poskytnutí slevy z ceny / uplatnění dvojí ceny v závislosti na uživatelském zadání koncového data pro poskytnutí slevy a současném zvolení druhu distribučního kanálu (e-shop, prodejní okénko).
6.11.2008	Dne 06.11.2008 byla doručena žádost DPP o opravu funkcionality DOS: Nezapsaný kupon do DB v případě duplikátu a žádost DPP o opravu funkcionality DOS: Provádět import dat z SKC automaticky, nikoli ručním spuštěním obsluhy back-office pracoviště DOS.
7.11.2008	Dne 07.11.2008 předal zástupce společnosti Haguess zástupci DPP instalační disky aplikace DOS, verze 1.0 a byla ukončena akceptace Aplikace DOS - Emulátor validátoru (tzv. lehké prodejní místo) dodané společností Haguess v souladu s žádostí o změnu funkcionality DOS č.6 ze dne 18.9.2008.
27.11.2008	Dne 27.11.2008 byla ukončena akceptace Aplikace DOS - Validátor.

4.1.5. Rok 2009

Datum	Fáze projektu
28.4.2009	Dne 28.04.2009 Byla předána do provozu aplikace DOS pro Validátor, verze 2.2.5 Předány byly: firmware čtečky, aplikační SW validátoru, WS a relevantní úpravy v DB DOS, instalační příručka. Součástí protokolu jsou: pokyny k nasazení ASW Validátor, Potřebné vybavení pro instalaci, Postup nahrání firmware.
1.6.2009	Dne 01.06.2009 byla v souladu se smlouvou o dílo ze dne 15.7.2008 a jejím dodatkem č.2 ze dne 22.12.2008 vystavena faktura č. FV-28/2009 za rozšíření funkcionality systému DOS na částku 4 800 000 Kč.

Vzhledem k neshodám v jednání mezi HMP a DPP o způsobu úhrady nákladů na zavedení projektu Opencard se DPP rozhodl, že projekt „zmrazí" v podobě, jak byl používán před dubnem 2009 a nebude pokračovat v jeho dalším rozvoji až do okamžiku, kdy dojde k dohodě s MHMP.

Současně jsme od DPP získali informaci, že pouze 260 tisíc z celkových 385 tisíc karet má nahraný některý z předplatných kupónů MHD, z čehož plyne, že určitá část karet byla uživateli pouze vyzvednuta a aktivována v roce 2008 v rámci dotované distribuce Opencard zdarma.

Výsledkem je, že část vynaložených nákladů na vydané karty a současně významná část licenčních poplatků je vynakládána aniž by dané Opencard využívaly jakoukoliv aplikaci a byly zapojeny do systému. Část těchto karet nebyla nikdy vyzvednuta. Další část byla vyzvednuta pouze z důvodu že HMP karty rozdávalo po určitou dobu zdarma, aniž by později došlo k jejich vlastnímu využití.

4.2. Použité vstupy, informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společností Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace s DPP
- Projektová dokumentace Soluziona

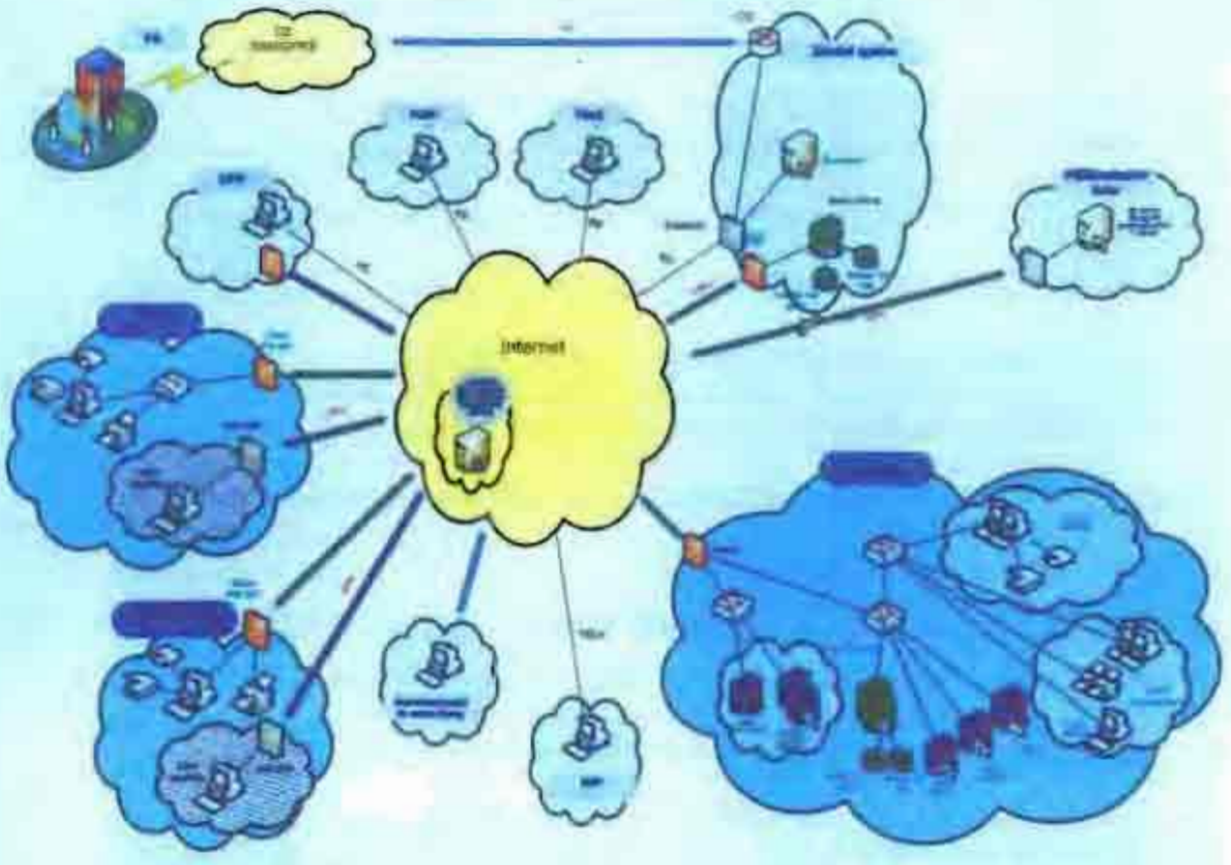
- Konzultace Deloitte
- Metodiky projektového řízení – Best Practices
- Veřejné informační zdroje

5. Posouzení technologické infrastruktury PCMS

Projekt Opencard je založen na vlastním řešení společnosti Haguess, které je současně i provozovatelem celého systému. Z tohoto pohledu je důležité, aby HMP mělo k dispozici kompletní dokumentaci, která se infrastruktury týká a pravidelně kontrolovala aktualizaci a dodržování bezpečnostní dokumentace a aby aktivně pracovala s risk managementem celého projektu. Z tohoto pohledu proběhlo ze strany HMP nejméně jednou ročně technologické posouzení projektu, které vedlo k identifikaci problémovým míst a jejich následnému dopracování ze strany společnosti Haguess.

V rámci posouzení, které jsme prováděli a podrobně zkontrolovali postup, který byl interně ve společnosti Haguess procesován od 1.4.2009, kdy proběhlo posouzení ze strany společnosti XEOS do 1.9.2009, kdy byly splněny všechny úkoly, a došlo ke kompletní revizi bezpečnostní dokumentace. Z pohledu našeho posouzení probíhal tento proces dle nastaveného harmonogramu a výsledné výstupy odpovídají závěrům, které byly 1.4.2009 společnosti Haguess předány. Před tímto posledním posouzením proběhlo ještě posouzení společnosti Deloitte v roce 2008 a společnosti Relsie v roce 2007.

5.1. Výchozí stav

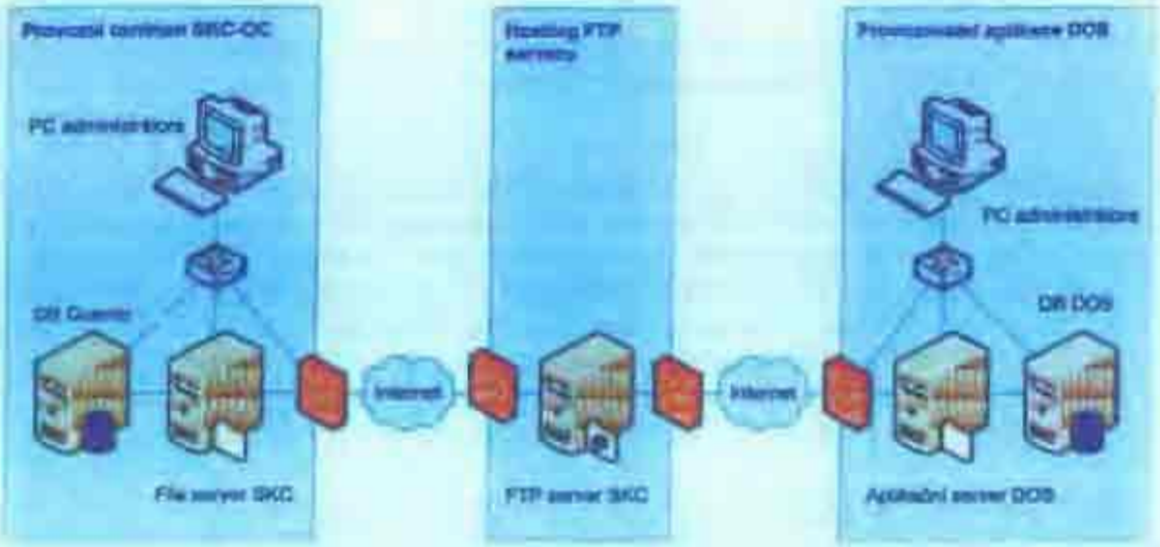


Obrázek – topologie systému.

5.2. Posouzení

Technologické posouzení infrastruktury PCMS

Architektura a proces výměny dat pro datovou komunikaci SKC – DOS



Obrázek - Fyzický model výměny dat mezi SKC a DOS

Databázový server Quanto a File server SKC jsou fyzicky oddělené servery, které jsou spolu s PC administrátora provozovány v jedné LAN provozovatele SKC-OC (Haguess). FTP server SKC je vyhrazen pro výměnu datových souborů s kartovými aplikacemi systému.

Opencard a je umístěn v hostingu s garantovanou dostupností služby 24x7.

- Provozní centrum SKC-OC společnosti Haguess, je fyzicky umístěno v Rosmarin Business Centrum, Dělnická 12, Praha 8.
- FTP server SKC je provozován v technologickém sále společnost Asseco, Podvinný mlýn 6, Praha 9.
- Provozovatelem kartové aplikace DOS je Dopravní podnik hl. města Prahy, a.s.

5.3. Průběh a zpracování výměny dat

Administrátor SKC-OC spouští proces zpracování blacklistu a datového souboru s typovými zprávami 1 x denně souhrnně pro všechny kartové aplikace evidované ke kartám v SKC-OC.

V rámci této úlohy vygeneruje systém SKC-OC oba soubory určené pro aplikaci DOS a uloží je jednak do složky na File serveru SKC a jednak do příslušných složek na FTP serveru SKC.

Systém SKC neodesílá aplikaci DOS žádné avízo o vytvoření a uložení nových souborů do složky DOS na FTP serveru.

Aplikační server DOS automaticky (bez zásahu administrátora DOS) kontroluje dostupnost nových souborů na FTP serveru SKC. Pokud aplikační server DOS zjistí, že ve složkách na FTP serveru je nový soubor (blacklist nebo datový soubor s typovými zprávami), stáhne jej do svého úložiště a soubor ze složky na FTP serveru smaže.

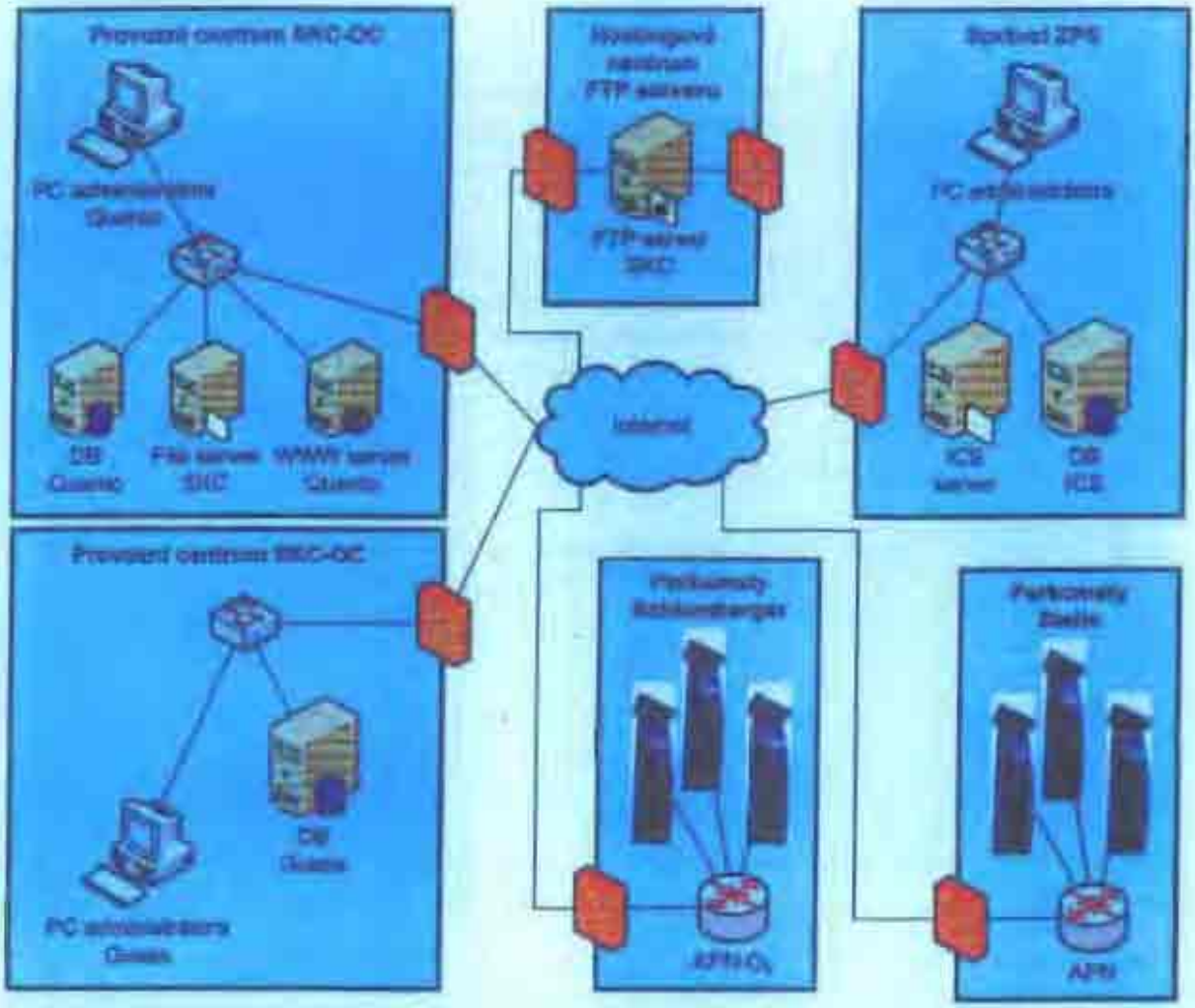
Na straně aplikace DOS je zpracování těchto souborů prováděno automaticky pomocí úlohy naplánované na aplikačním serveru DOS (s doporučeným intervalem 6 hodin, tj. 4x denně).

Zpracování je rozděleno do dvou kroků; v prvním kroku se příslušné soubory přenesou z FTP serveru SKC do lokálního souborového systému serveru (a smažou se na FTP serveru SKC), ve druhém kroku se příslušné soubory zpracují a příslušné informace se zapíšou do centrální databáze aplikace DOS. V případě, že se některý soubor podaří zpracovat jen částečně nebo vůbec, je umístěn do speciální složky v rámci DOS. Administrátor aplikace DOS složku týdně (podle potřeby i častěji) kontroluje a nezpracované soubory řeší.

Příčin nezdařeného importu souborů na straně provozovatele aplikace DOS může být více. Administrátor DOS má možnost vyžádat si u administrátora SKC opětovné zasláni příslušných souborů. V SKC jsou tyto soubory uloženy jednak na File serveru a jednak v historii cca 14 dnů v DB Quanto (pouze blacklisty).

5.4. Architektura a proces výměny dat pro datovou komunikaci SKC – KAP

Výměna datových souborů mezi SKC-OC a aplikací KAP je provozována v následujícím fyzickém modelu komunikační sítě:



Obrázek - Fyzický model výměny

Fyzický model výměny dat mezi SKC a KAP Databázový server Quanto, databázovýserver Guess, File server SKC a WWW server Quanto jsou fyzicky oddělené servery, které jsou spolu s PC administrátora Quanto a Guess provozovány v jedné LAN provozovatele SKC-OC (Haguess).

FTP server SKC je vyhrazen pro výměnu datových souborů s kartovými aplikacemi systému Opencard a je umístěn v hostingu s garantovanou dostupností služby 24x7.

- Provozní centrum SKC-OC společnosti Haguess, je fyzicky umístěno v Rosmarin Business Centrum, Dělnická 12, Praha 8.

- FTP serveru SKC je provozován v technologickém sále společnost Asseco, Podvinný mlýn 6, Praha 9.
- ICS servery jsou fyzicky umístěny v sídlech provozovatelů jednotlivých správců ZPS. Prostřednictvím ICS serverů je řízena datová výměna s parkomaty značky Stello.
- Parkomaty značky Schlumberger přistupují a svá data sdílejí přímo s FTP serverem SKC.

Administrátor SKC-OC spouští proces zpracování blacklistu 1 x denně, souhrnně pro všechny kartové aplikace evidované ke kartám v SKC-OC. V rámci této úlohy vygeneruje systém SKC-OC soubor blokovaných karet pro aplikaci KAP. Tento soubor uloží do složky na File serveru SKC a dále jej rozkopíruje do složek na FTP serveru SKC.

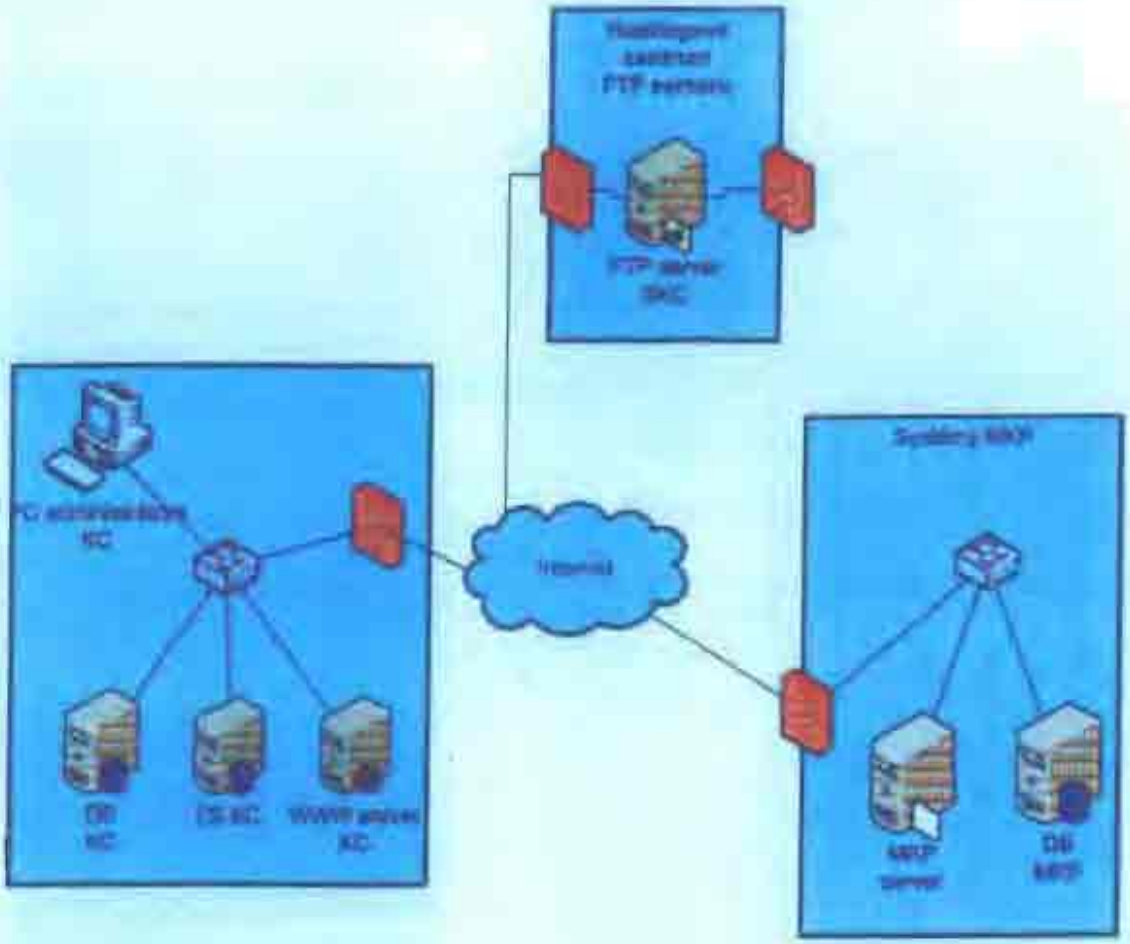
Systém SKC neodesílá aplikaci KAP žádné avízo o vytvoření a uložení nových souborů do složek na FTP serveru. Nové soubory se do složek jednotlivých provozovatelů pouze přidávají, staré soubory zůstávají zachovány pro případ nezdařeného importu na straně provozovatele parkomatů.

ICS servery se automaticky v určený čas připojí k FTP serveru a zjistí existenci nového blacklistu. Pokud ICS server zjistí, že ve složkách na FTP serveru je blacklist, stáhne jej do svého úložiště a soubor ve složce na FTP serveru ponechá. Parkomaty značky Schlumberger nekomunikují prostřednictvím ICS serveru, nýbrž sdílejí data napřímo s FTP serverem SKC.

Jelikož administrátorská pracoviště a databázové stroje systémů Guess a Quanto jsou fyzicky oddělená pracoviště, probíhá zjišťování informací o platnosti karet dotazem na webovou službu běžící nad Centrem sdílených služeb. Pracoviště administrátorů aplikace Guess a Quanto jsou sice provozovány v jedné LAN síti, ale nastavení rolí a přidělení oprávnění je pro každou aplikaci nezávislé.

5.5. Architektura a proces výměny dat pro datovou komunikaci SKC – MKP

Výměna datových souborů mezi SKC-OC a aplikací MKP je provozována v následujícím fyzickém modelu komunikační sítě:



Obrázek - Fyzický model výměny dat mezi SKC a MKP

Databázový server Quanto a File server SKC jsou fyzicky oddělené servery, které jsou spolu s PC administrátora provozovány v jedné LAN provozovatele SKC-OC (Haguess). FTP server SKC je vyhrazen pro výměnu datových souborů s kartovými aplikacemi systému Opencard a je umístěn v hostingu s garantovanou dostupností služby 24x7.

- Provozní centrum SKC-OC společnosti Haguess, je fyzicky umístěno v Rosmarin Business Centrum, Dělnická 12, Praha 8.
- FTP server SKC je provozován v technologickém sále společnost Asseco, Podvinný mlýn 6, Praha 9.
- Provozovatelem kartové aplikace MKP je Městská knihovna Praha

5.6. Proces výměny dat pro datovou komunikaci SKC – Portál HMP

Administrátor SKC-OC spouští proces zpracování datového souboru s typovými zprávami 1 x denně souhrnně pro všechny kartové aplikace evidované ke kartám v SKC-OC. V rámci této úlohy vygeneruje systém SKC-OC soubor určený pro aplikaci Portál HMP, uloží je do složky „OUT" určené pro aplikaci Portál HMP na File serveru SKC a odešle prostřednictvím aplikace CURL.

Aplikační server Portál HMP obratem odpoví odesláním datového souboru s typovými zprávami a elementem <ZARAZENO> TRUE </ZARAZENO>. Tento soubor je uložen do složky „IN" určené pro aplikaci Portál HMP na File serveru SKC a automaticky zpracován.

5.7. Použité vstupy, informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společností Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace s DPP
- Projektová dokumentace Soluziona
- Konzultace Deloitte
- Metodiky projektového řízení - Best Practices
- Veřejné informační zdroje

6. Vhodnost vybraných technologií, vhodnost jejich kombinací a dodržení standardů

6.1. Výchozí stav

Systém byl na počátku spuštěn s hybridní kartou MIFARE Classic i přesto, že v době spuštění již byla na trhu jiná, bezpečnější řešení včetně později použité MIFARE DESFire. Cenové hledisko, které by mohlo být hlavním a jediným důvodem pro tuto volbu se na základě zkoumání ukázalo jako irelevantní, jelikož již v rámci počáteční fáze projektu bylo definováno, že je nutné nakoupit čtečky, které podporují jak MIFARE Classic, tak MIFARE DESFire. Současně bylo zbytečně pořízeno celkem 50 000 karet MIFARE DESFire, z nichž bylo nakonec použito pouze necelých 10%.

Zavedení dvou různých karet znamenalo pro technologickou platformu PCMS dva různé způsoby komunikace karty s aplikací a také, vzhledem k tomu, že nová karta MIFARE DESFire obsahuje operační systém a šifrovací mikročip, zdvojení dalších vyvíjených prvků systému, jakými jsou oblast bezpečnosti, způsob ukládání dat na kartu apod.

Druhým problémem nákupu hybridní karty je fakt, že hybridní karta, tedy karta, které obsahuje jak bezkontaktní, tak kontaktní čip, nebyla nikdy v plné šíři využita, jelikož kontaktní čip lze v tuto chvíli použít hlavně k počítačové identifikaci, které však funguje pouze pro aplikaci „Vím jak řídím". Pokud by došlo k zavedení karet obsahujících POUZE bezkontaktní čip, došlo by k výrazné úspoře nákladů, jelikož běžná karta je oproti hybridní kartě o polovinu levnější.

6.2. Posouzení

Volbě zvolené technologie předcházela analýza s názvem „Koncepce centra karetních a platebních služeb HMP", kterou na základě smlouvy z roku 2005 vypracovala pro odbor informatiky společnost Soluziona, a.s.

Použití původní technologie MIFIRE Classic pro pilotní provoz a jeho následné nahrazení technologií MIFIRE DESFire je v souladu s původní předprojektovou studií společnosti Soluziona „Pražské centrum kartových služeb" datovanou do roku 2005. Z tohoto pohledu konstatujeme, že problém změny karetní technologie přisuzujeme špatnému projektovému rozhodnutí v době realizace projektu, kdy se podmínky nasazování jednotlivých typů karet od původní studie změnily.

Volba karty MIFIRE Classic pro pilotní projekt, namísto v době již běžně využívané karty MIFARE DESFire pak v konečném důsledku znamenala zbytečně vynaložené náklady na pořízení karet, které nebyly nikdy využity, a současně vedla k placeným úpravám celého systému. Do zadávací dokumentace byl zakotven požadavek na karty MIFARE Classic a následně pak do smlouvy se společnosti Haguess zapracován požadavek na nákup 50 000 ks hybridních karet s bezkontaktním čipem MIFARE

Classic, které MHMP nakoupil v roce 2006 za cenu 18,9 mil. Kč vč. DPH. Většina z těchto karet, konkrétně více jak 90% je stále uložena bez jakéhokoliv plánu na využití u dodavatele a jejich budoucí využití je spíše v teoretické rovině, jelikož od července 2008 došlo ke dvěma významným změnám: karty s čipem MIFARE Classic byly nahrazeny kartami MIFARE DESFire a současně došlo k posunu v požadavcích tak, že namísto hybridních karet jsou využívány karty, které obsahují pouze bezkontaktní čip, které jsou významně levnější.

MHMP tak vznikl zbytečný náklad na pořízení hybridních karet MIFARE Classic, který bude pravděpodobně nutné odepsat. Následná změna technologie v průběhu projektu stála v roce 2007 dle dostupných údajů částku 19 mil Kč včetně DPH. Část výše uvedených nákladů měla nebo mohla být uspořena, pokud by odbor informatiky MHP respektoval odborná doporučení, lépe vyhodnotil počet karet pro pilotní provoz, nebo pokud by disponoval odborným zázemím pro takováto technologická rozhodnutí. Odborné zázemí lze kromě komerční sféry získat například na akademické půdě. Současně jsme dospěli k závěru, že v období listopadu 2006 až duben 2007 měla tuto odbornou stránku zajišťovat v roli projektového managementu společnost Soluziona, které zpracovávala původní koncepci a mohla tedy s využitím této znalosti z pozice projektového řízení, které si odbor informatiky na projekt smluvně najal, ovlivňovat, případně na nesoulady upozornit, o čemž jsme však žádné záznamy nenašli.

Podobně by bylo možné očekávat při tak významných částkách a při tak rozsáhlém projektu očekávat od dodavatele, že na možné riziko související s volbou MIFARE Classic a s nákupem 50 000 karet upozorní, případně, že MHP předloží vlastní technologický návrh, který by zamezil zbytečnému vynakládání prostředků v rámci projektu. Dalším možností minimalizace této ztráty mohlo být dodržení propagačních a marketingových aktivit, které předpokládaly vyšší rozšíření karet mezi uživatele již v pilotním provozu. U tohoto kritéria však zdůrazňujeme, že velký časový odstup snižuje možnost detailně vyhodnotit, zda bylo možné stávající stav v době řešení ovlivnit.

6.3. Použité vstupy, informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společností Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace s DPP
- Projektová dokumentace Soluziona
- Konzultace Deloitte
- Metodiky projektového řízení – Best Practices
- Veřejné informační zdroje

7. Licenční politika, ochrana vlastnických práv, záruční podmínky

7.1. Výchozí stav

Základní rámec licenční politiky a ochrany vlastnických práv je definován v těchto dokumentech:

Předně tedy v Základní smlouvě ze dne 27.10.2006, mezi MHMP a Haguess, DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra, včetně jejích dodatků. Dále je zde seznam dalších smluv, vycházejících z této základní smlouvy a které jsou evidované odborem informatiky MHMP.

Číslo smlouvy	Název smlouvy	Datum	Subjekt
DIL/40/05/001120/2006	Vytvoření Servisního Kartového Centra	27.10.2006	HGS
INO/40/05/001127/2006	Servisní smlouva příloha k 1120/2006	6.11.2006	HGS
LIC/40/05/001128/2006	Licenční smlouva příloha k 1120/2006	6.11.2006	HGS
USC/40/05001153/2006	Smlouva o úschově	11.12.2006	HGS
INO/40/05/001270/2007	Dodávka licence Kartové aplikace parkování	26.2.2007	HGS
DIL/40/05/001271/2007	Servis. podpora IS Kartové apl. Parkování	26.2.2007	HGS
INO/40/05/001296/2007	Smlouva o zajištění provozu PCKS -1.4.2007-30.9.2007	12.4.2007	HGS
INO/40/01/001386/2007	Smlouva o zajištění provozu PCKS -1.11.2007-31.7.2008	31.10.2007	HGS
DIL/40/01/001529/2008	Licence kartového aplikace parkování „KAPII"	21.4.2008	HGS
LIC/40/01/001613/2008	Licenční smlouva - závazek ze sml 1120/2006, resp 1128/2006	14.7.2008	HGS
DIL/40/01/001652/2008	Rozšíření SKC o technologii MIFARE DESFire	31.7.2008	HGS
INO/40/01/001638/2008	Smlouva o zajištění provozu PCKS -1.8.2008-31.12.2008	31.7.2008	HGS

LIC/40/01/001650/2008	Licenční smlouva	31.7.2008	HGS
DIL/40/01/001684/2008	Provozování kartové aplikace s využitím karty Opencard	31.7.2008	DPP
INO/40/01/001831/2009	Smlouva o zajištění provozu PCKS -1.1.2009-28.2.2009	2.1.2009	HGS
INO/40/01/001860/2009	Smlouva o zajištění provozu PCKS -1.3.2009-30.4.2009	26.2.2009	HGS
INO/40/01/001966/2009	Smlouva o zajištění provozu PCKS -1.5.2009-31.8.2009	25.5.2009	HGS
DIL/40/01/001684/2008	Smlouva o umožnění provozování kartové aplikace s využitím karty Opencard	31.7.2009	DPP

7.2. Posouzení

Předmětem posouzení je základní rámec licenční politiky a ochrany vlastnických práv zadavatele MHMP. Tato problematika je pojmenována v Základní smlouvě ze dne 27.10.2006, mezi MHMP a Haguess, DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra, včetně jejích dodatků a pak ve smlouvách uzavřených následně.

Licence, vlastnická práva:

Licenční smlouva nebyla uzavřena zároveň se Základní smlouvou ze dne 27.10.2006, mezi MHMP a Haguess, DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra.

Licenční smlouva byla uzavřena následně a to 6.11.2006, mezi MHMP a Haguess, DIL/40/05/001128/2006.
Licenční smlouva DIL/40/05/001128/2006 se stala Přílohou č.7 smlouvy Základní DIL/40/05/001120/2006.

Licenční smlouva je uzavřena na dobu neurčitou dle článku II.4. Licenční smlouva definuje typ a rozsah poskytnuté licence a to zejména v článku III.1. licence typu B.1.1 s horním limitem 100 tisíc karet.

Licence na Software SKC je poskytována vždy časově neomezená, nepřenositelná a nevýhradní (Příloha č.1, Přílohy č.7).
Součástí licence Aplikace SKC nejsou zdrojové kódy.

Licence Aplikace SKC obsahuje SW produkty, jenž tvoří jeden funkční konfigurovatelný celek:

- KRONUS - univerzální řídicí systém
- QUANTO – systém pro správu karet (CMS)
- KWADROM - datový zúčtovací systém
- CHANSON - zázemí elektronické peněženky

Licence na Aplikace SKC je poskytována v závislosti na třech parametrech:

- Počet evidovaných karet v Aplikacích SKC (do 100 tis)
- Počet konfigurovaných uživatelských stanic v Aplikacích SKC (do 15)
- Počet kartových aplikací integrovaných v Aplikacích SKC (do 5)

Cena za licence je poskytnuta v rámci celého kontraktu (III.2.), avšak zadávací dokumentace k výběrovému řízení na Vytvoření SKC nehovořila o žádném horním limitu (licenčním). Vycházíme-li z počtu stávajících uživatelů služeb MHD DPP – předplatitelé měsíčních, čtvrtletních a ročních kupónů, kterých je cca 660 tisíc (v roce 2006 to byl obdobný počet).
Je zde disharmonie. Následně, v jednacím řízení bez uveřejnění, byl zvýšen limit pro počet karet v systému na 200 tis karet, 45 uživatelských stanic a 5 aplikací.

HMP v licenčním modelu zcela přistoupilo na nabízený licenční model, aniž by proběhla odborná oponentura, zda je pro HMP takový model akceptovatelný a výhodný. Pokud by v počáteční fázi projektu HMP lépe hájilo své zájmy, byly by pravděpodobně licenční podmínky nastaveny tak, aby nedocházelo k duplicitnímu, a neefektivnímu započítávání licencí karet, které aktivně systém nevyužívají nebo nebudou využívat.

V Příloze č.1, přílohy č.7 Licenční smlouvy DIL/40/05/001128/2006 je zpoplatněn limit počtu karet, v tomto případě licence typu B.I.1. 100 tis karet, a pak zvláště jsou zpoplatněny kartové aplikace v systému SKC.

Negativním faktorem je ta skutečnost, že jsou zpoplatněny i neaktivní karty v systému.

Veškerá vlastnická, jakož i autorská práva jsou společnosti Haguess a MHMP má jen licenčně propůjčeno k užívání, tudíž MHMP není vlastníkem licencí.

Vlastnická práva k licencím:

- Dodavatel je výhradním vlastníkem
- Objednatel má jen propůjčené právo k užívání
- Není umožněn provoz prostřednictvím třetí osoby

Příloha č.1, Přílohy č.7 Licenční smlouvy DIL/40/05/001128/2006: Poskytovatel (Haguess) prohlašuje a zaručuje, že je výrobcem a výhradním majitelem Software SKC a oprávněnou osobou k nakládání s autorskými právy vztahujícími se k Software SKC, a že je oprávněn poskytovat licenci k využívání Software SKC v souladu se zadávací dokumentací a v souladu s touto Licenční smlouvou nabyvateli.

Licenční politika je pak ve smlouvách následných identická, je zachována ve stejných intencích jako se smlouvou základní ze dne 27.10.2006, mezi MHMP a Haguess, DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra.

MHMP je závislý na jednom exkluzivním dodavateli. Nelze například uskutečnit otevřenou, transparentní soutěž na dodavatele. MHMP nedostatečně odhadl, na počátku projektu (2006), důsledky zvolené licenční politiky a současně, v průběhu projektu, důsledně neprosazoval své zájmy v tomto projektu, tak aby došlo k nápravě licenčního vztahu do podoby, z níž by profitovaly obě strany (princip vztahu win - win).

Používaný licenční model je jednostranně nastaven na maximalizaci výnosů a ochranu zájmů dodavatele Haguess. Jedna ze základních chyb vznikla již při zadávacím řízení, kdy MHMP nedefinoval, ani následně nejednal o preferovaném způsobu plnění zakázky (např: dodávka na klíč, customizovaný vývoj, outsourcing, licence, ...).

Nad rámec rozsahu zpracovaného posouzení, které je ohraničeno dnem 30.6.2009 konstatujeme, že dle získaných podkladů z jednání zastupitelstva HMP, které se konalo dne 17.12.2009, prezentoval zastupitel JUDr. Tomáš Homola, předseda výboru pro informatiku HMP, skutečnost, že bylo na výborech pro informatiku celkem opakovaně řešeno možné vypovězení smluv s dodavatelem Haguess. V této souvislosti se řešilo se i případné riziko totálního zmaření investice. Na jednání zastupitelstva bylo téma Opencard projednáváno, dle dostupných informací, pouze dvakrát. Z této informace vyplývá, že minimálně část MHMP dlouhodobě poukazovala na nevýhodnost smluvního vztahu souvisejícího s projektem Opencard a dle získaných podkladů nejméně od konce roku 2008 probíhala jednání, která byla směřována k nápravě stavu, bohužel se první dílčí změny podařily vyjednat až v prosinci 2009 (prvním náměstkem primátora JUDr. Rudolfem Blažkem).

Záruka:

Záruční podmínky jsou v souladu se zákonem a jsou definovány v Příloze č.7 – vzor licenční smlouvy (Licenční smlouva DIL/40/05/001128/2006) Příloha č.7 je součástí smlouvy DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra.

Záruční podmínky jsou pojmenovány zejména v článku:
VII.2. Poskytovatel poskytuje Nabyvateli záruku na program SKC po dobu trvání záruční lhůty. Záruční lhůta činí 24 měsíců ode dne prodeje licence na Software SKC.
VII.5. Poskytovatel poskytuje záruku na funkčnost Software SKC.
VII.6. Záruční doba počíná běžet dnem předání Software SKC podle této smlouvy.

Záruky jsou tudíž v pořádku a jsou obvyklé dodávkám obdobného charakteru.

Pojištění

V rámci zadání výběrového řízení na „SKC" v roce 2006, bylo požadováno pojistné plnění z odpovědnosti dodavatele. Dodavatel tuto pojistnou smlouvu uzavřel s Českou pojišťovnou s účinností od 1.9.2006 do 31.8.2007. Výše plnění byla 10 miliónů Kč. V následně uzavřených kontraktech byla výše pojistného plnění z odpovědnosti navýšena na 25 miliónů Kč.

Toto plnění z odpovědnosti dodavatele je doposud platné. Zadavatel MHMP, s péčí řádného hospodáře, adekvátně ošetřil toto riziko.

Posouzení:

- Požadavek na způsob dodávky nebyl součástí zadání (dílo, licence, customizace, outsourcing)
- Licenční poplatky se samostatně vztahují na systémy:
  - DOS (dopravní odbavovací systém)
  - SKC (servisní kartové centrum), podhodnocen objem emitovaných karet pro 100 tisíc uživatelů Opencard
  - KAP (kartová aplikace parkování)
- Nebyl brán zřetel na optimální počet uživatelů shodný s počtem občanů města Prahy, včetně „dojížděcích" občanů za prací, studiem a turistikou. Současný kmen veškerých předplatitelů MHD DPP je cca 660 tisíc.
- Zpoplatněny veškeré karty evidované v systému, bez zohlednění aktivní či neaktivní karta
- Ochrana vlastnických práv

Doporučení - směry:

- Zásadním způsobem přehodnotit licenční politiku dodavatele s cílem:
  - Sjednotit (paušalizovat) poplatek za jednoho unikátního uživatele v systému PCMS (nyní uživatel může mít vícero karet v systému)
  - Sjednotit licenční politiku pouze na PCMS (eliminovat samostatné licencování DOS, SKC, KAP a případně dalších aplikačních řešení, systémů)
  - Zpoplatnit pouze aktivní uživatele v systému PCMS
  - Případně přejít na formu multilicenční politiky a tím mimo jiné docílit omezení administrativy projektu (měsíční statistiky uživatelů OC a následné fakturace)

Z důvodu:

- Nepřiměřené finanční zátěže pro zadavatele MHMP, s progresivním růstem nákladů, dle počtu uživatelů v systému PCMS.

7.3. Použité vstupy, informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společností Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace s DPP
- Osobní konzultace s odborem legislativy MHMP
- Osobní konzultace s právní kanceláří Randa Legal
- Konzultace Deloitte
- Zákony o veřejných zakázkách a to zákon č.40/2004 Sb. a zákon č.137/2006 Sb.
- Obchodní zákoník
- Veřejné informační zdroje

8. Rozsah prací, následná údržba PCMS

8.1. Výchozí stav

Základní rámec je definován v těchto dokumentech (pouze MHMP):

Předně tedy v Základní smlouvě ze dne 27.10.2006, mezi MHMP a Haguess, DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra, včetně jejích dodatků. Dále je zde seznam dalších smluv, vycházejících z této základní smlouvy a které jsou evidované odborem informatiky MHMP.

Číslo smlouvy	Název smlouvy	Datum	Subjekt
DIL/40/05/001120/2006	Vytvoření Servisního Kartového Centra	27.10.2006	HGS
INO/40/05/001127/2006	Servisní smlouva příloha k 1120/2006	6.11.2006	HGS
LIC/40/05/001128/2006	Licenční smlouva příloha k 1120/2006	6.11.2006	HGS
USC/40/05001153/2006	Smlouva o úschově	11.12.2006	HGS
INO/40/05/001270/2007	Dodávka licence Kartové aplikace parkování	26.2.2007	HGS
DIL/40/05/001271/2007	Servis. podpora IS Kartové apl. Parkování	26.2.2007	HGS
INO/40/05/001296/2007	Smlouva o zajištění provozu PCKS - 1.4.2007-30.9.2007	12.4.2007	HGS
INO/40/01/001386/2007	Smlouva o zajištění provozu PCKS - 1.11.2007-31.7.2008	31.10.2007	HGS
DIL/40/01/001529/2008	Licence kartového aplikace parkování „KAPII"	21.4.2008	HGS
LIC/40/01/001613/2008	Licenční smlouva - závazek ze sml 1120/2006, resp 1128/2006	14.7.2008	HGS

DIL/40/01/001652/2008	Rozšíření SKC o technologii MIFARE DESFire	31.7.2008	HGS
INO/40/01/001638/2008	Smlouva o zajištění provozu PCKS - 1.8.2008-31.12.2008	31.7.2008	HGS
LIC/40/01/001650/2008	Licenční smlouva	31.7.2008	HGS
DIL/40/01/001684/2008	Provozování kartové aplikace s využitím karty Opencard	31.7.2008	DPP
INO/40/01/001831/2009	Smlouva o zajištění provozu PCKS - 1.1.2009-28.2.2009	2.1.2009	HGS
INO/40/01/001860/2009	Smlouva o zajištění provozu PCKS - 1.3.2009-30.4.2009	26.2.2009	HGS
INO/40/01/001966/2009	Smlouva o zajištění provozu PCKS - 1.5.2009-31.8.2009	25.5.2009	HGS
DIL/40/01/001684/2008	Smlouva o umožnění provozování kartové aplikace s využitím karty Opencard	31.7.2009	DPP

8.2. Posouzení

Předmětem posouzení je rozsah prací a následná údržba. Rámec smluvního vztahu určuje Základní smlouva ze dne 27.10.2006, mezi MHMP a Haguess, DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra, včetně jejich dodatků.

Následná údržba

Pod tímto pojmem shledáváme tyto činnosti:

- Zajištění provozu
- Servisní podpora

Podpora a údržba systému je v souladu se zákonem a je definována v Příloze č.6 – vzor servisní smlouvy (Servisní smlouva DIL/40/05/001127/2006).
Příloha č.6 je součástí smlouvy DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra.

Dále pak ve smlouvách:

- INO/40/01/001386/2007 Smlouva o zajištění provozu PCKS - 1.11.2007-31.7.2008
- INO/40/01/001638/2008 Smlouva o zajištění provozu PCKS - 1.8.2008-31.12.2008
- INO/40/01/001831/2009 Smlouva o zajištění provozu PCKS - 1.1.2009-28.2.2009
- INO/40/01/001860/2009 Smlouva o zajištění provozu PCKS - 1.3.2009-30.4.2009
- INO/40/01/001966/2009 Smlouva o zajištění provozu PCKS - 1.5.2009-31.8.2009
- DIL/40/05/001120/2006 Vytvoření Servisního Kartového Centra
- DIL/40/05/001271/2007 Servis. podpora IS Kartové apl. parkování
- INO/40/05/001296/2007 Smlouva o zajištění provozu PCKS - 1.4.2007-30.9.2007

Servisní smlouva DIL/40/05/001127/2006 určuje:

- Dobu plnění, tj. 4 roky od ukončení zkušebního provozu
- Předmět plnění
- Rozsah servisních služeb a jejich reakční doby
- Komunikační rozhraní
- Práva a povinnosti obou smluvních stran
- Sankční ujednání – smluvní pokuty, jenž jsou přiměřené plněním obdobného charakteru.

Následné servisní smlouvy či smlouvy o provozu, rozšířili smluvní ujednání o činnosti typu:

- Technicko - organizačních opatřeních pro nakládání s osobními daty
- Platnost karty 4 roky
- Dohodu o provozu kontaktních míst
- Garantovanou dostupnost systému 96,5 % v kalendářním roce

Podpora a údržba systému je obvyklá dodávkám obdobného charakteru – rozsahem a danými parametry služby. Avšak díky špatně nastavené licenční politice (2006) je zde zřejmý neúměrný nárůst ceny za službu jako takovou.

Rozsah prací

Systémy s nimiž jsme se seznámili:

- KRONUS - univerzální řídicí systém
- QUANTO - systém pro správu karet (CMS)
- KWADROM - datový zúčtovací systém
- CHANSON - zázemí elektronické peněženky

Hodnocení jejich pracnosti je v kontextu zakázky irelevantní, jelikož HMP přistoupilo na licenční model (2006) a relevantním ukazatelem by tedy měla být cena za poskytnutou licenci. Společnost Haguess kromě možné přímo hodnotitelné pracnosti uvádí ještě předchozí vývoj a koncept s počátky od roku 2003. Vzhledem k licenčnímu modelu prodeje, nemá HMP k dispozici zdrojové kódy, ani datové struktury, které by mohly být podkladem pro hodnocení pracnosti.

V rámci posouzení jsme absolvovali i prezentaci systému Guess, Kwadrom, Chanson s tím, že nám byla předvedena prezentační vrstva, tedy uživatelský interface a ostatní části systému byly popsány jen verbálně a ve formě běžné projektové dokumentace. Technická část dokumentace není v rámci projektu k dispozici, jelikož smluvně jde o licenční model, v rámci něhož není významná část technických informací poskytována.

8.3. Použité vstupy, informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společností Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace DPP
- Osobní konzultace s odborem legislativy MHMP
- Osobní konzultace s právní kanceláří Randa Legal
- Konzultace Deloitte
- Zákony o veřejných zakázkách a to zákon č.40/2004 Sb. a zákon č.137/2006 Sb.
- Obchodní zákoník
- Veřejné informační zdroje

9. Identifikace a stručný popis významných technologických, případně systémových chyb a nedostatků v dosavadní realizaci projektu Opencard

9.1. Posouzení

9.1.1. Předpokládaný podnikatelský plán

Projekt Opencard byl ze současného pohledu nastaven a následně i schválen v optimistickém předpokladu, který vycházel z nereálných ekonomických a finančních parametrů. Prvotní studie „Využití čipové karty v podmínkách HMP" předložená společností Allshare Finance a která byla předložena zastupitelstvu dne 25.5.2006, nastavila podnikatelský plán s návratností do roku 2015. Projekt sice počítal s kartami zdarma pro pilotní projekt (2006), ale nepočítal s následnou distribucí karet zdarma i v reálném provozu. Příjem z prodeje karet měl dle předloženého podnikatelského plánu pokrývat celkem 80% z příjmů projektu. Současně však plánoval první příjmy již v roce 2007, což bylo z pohledu v podstatě ročního termínu od studie nereálné z mnoha důvodů.

Podnikatelský plán nastavoval i další parametry plánovaných příjmů: provize z transakcí 2,2 - 3%, poplatek za dobíjení 9-25Kč, prodej karet za 210 - 250/kus s platností 2 roky, příjem HMP ve výši 2% z termínovaného depozitu, který by v podstatě obhospodařoval peníze uložené na kartách. Vzhledem k neexistenci strategického partnera, který by zajistil bankovní licenci, však nemohla být příjmová položka z poplatků naplněna a pro získání kmenu 385 000 uživatelů byla zvolena strategie poskytování karet i v běžném provozu zdarma s platností na 4 roky, z čehož plyne, že nejdříve za 4 roky od vydání lze počítat s významnějšími příjmy z prodeje karet (tedy roku 2012).

9.1.2. Licence

Obecně platí, že licenční model je zvolen v případě, pokud dodavatelská firma vyvine software pro řadu zákazníků a ti, kteří jej chtějí používat si pořizují licenci. Pokud je významná část softwarového produktu plně vyvinuta za peníze zadavatele, je licenční způsob poskytování softwarového produktu nemorální. Licenční poplatky standardních softwarových balíků obsahují zároveň údržbu, rozvoj a servis k dodanému SW, ale v takovém případě obvykle nedochází k tomu, aby kromě licenčních poplatků byly čerpány další částky na vývoj dalších komponent systému.

Při posouzení jsme dospěli k závěru, že nejméně vybudování aplikace DOS, vykazuje rysy spíše dovývoje ke stávajícímu systému než licencování existující funkcionality stávajícího systému a v tomto bodě se neztotožňujeme se závěry znaleckého posudku podaného Ing. Kroupou, které by mohly vyznít jinak při odlišně položených otázkách. Nemorálnost uvedená v tomto odstavci nikterak neomezuje způsob, jakým mohou být

nastaveny smluvní vztahy mezi dodavatelem a objednatelem, pouze upozorňujeme na obvyklé postupy v dané oblasti.

9.1.3. Elektronická peněženka

V rámci projektu Opencard bylo uvažováno o elektronické peněžence, jako o jedné z klíčových aplikací. Vzhledem k tomu, že MHMP zatím nepodepsalo dohodu se strategickým partnerem, který by tuto aplikaci zastřešil bankovní licencí, došlo ke stavu, v němž není aktuálně spuštěna aplikace související s elektronickou peněženkou a žádná karta nemá tuto aplikaci aktivovanou.

Aplikace pro elektronickou peněženku byla v prvopočátku projektu používána pro zúčtování parkovacích transakcí, postupnými kroky však byla k 30.6.2008 zastavena a neobsahuje žádné údaje. Zúčtování parkovacích transakcí probíhá ve zjednodušeném režimu, kdy jsou všechny vybrané peníze rovnou převáděny MHMP.

9.1.4. Uživatelská přívětivost

I přesto, že jsme zkoumali technologické, organizační a bezpečnostní důvody stávajícího nastavení jednotlivých scénářů a postupů, které projekt Opencard nastavuje a chápeme jejich odůvodnitelnost za stávajícího stavu, zaměřili jsme své zkoumání i na oblast uživatelské přívětivosti celého systému pro občana, jelikož jde o jeden z klíčových aspektů, který rozhodne o masovém rozšíření projektu mezi obyvatele a návštěvníky HMP. V této oblasti jsme identifikovali množství podnětů, které lze řešit pro uživatele jednodušším způsobem. Jedním z příkladů je nutnost vložení předplacené částky pro aplikaci parkování pouze na kontaktních místech, což jednoznačně limituje dostupnost služby jako takové.

Podobně elektronických obchod DPP neposkytuje uživateli informaci o jeho předchozím (stále ještě platném) kupónu a uživatel si musí tuto informaci evidovat individuálně, což je například při využívání ročních nebo tříměsíčních předplatních kupónů velmi nepohodlné. Často tak může nastat situace, že si uživatel nakoupí kupón, který se několika dny překrývá s původním kupónem. Scénář, kdy si uživatel přečte u validátoru termín platnosti, vrátí se domů, nakoupí kupón v elektronickém obchodě DPP a následně si jde kupón „nabít" do karty je velmi neefektivní a pravděpodobně je to i jeden z důvodů, proč je na prodejních místech prodáno za rok 2009 celkem 508 577 elektronických předplatních kupónů a v elektronickém obchodně DPP pouze 70 674 elektronických předplatních kupónu. Určitou část tohoto poměru samozřejmě určují uživatelé, kteří nechtějí platit platební kartou v elektronickém obchodě, ale hlavním faktorem je pravděpodobně srovnání procesů obou způsobů koupě elektronických předplatních kupónů, z nichž jednodušeji vychází nákup v prodejních místech.

Vedlejším efektem tohoto stavu jsou dlouhé čekací doby u prodejních míst, nervozita a nespokojenost uživatelů. Celkově doporučujeme, aby v rámci projektu byly uživatelské scénáře posuzovány jako jedno z klíčových kritérií při nasazení jakékoliv služby.

9.1.5. Hodnocení řízení rizik, bezpečnost a business continuity

V rámci zkoumání bezpečnostních standardů, řízení rizik a business kontinuity jsem dospěli k závěru, že HMP nejméně jednou ročně provádí prostřednictvím třetích osob prověření bezpečnosti systémů souvisejících s Opencard a kontroluje bezpečnostní dokumentaci se systémy související, přesto je nutné podotknout, že se v této oblasti a dále v oblastech řízení rizik a business kontinuity plně spoléhá na dodavatele, například na rozdíl od DPP, který má vlastní pravidla, do nichž zapracována pravidla HGS.

9.1.6. Procesní – realizace projektu PCMS:

Projekt „Servisního kartového centra" (taktéž PCMS) byl vyhlášen zadáním veřejné zakázky na služby formou otevřeného řízení podle tehdy platného zákona č. 40/2004 Sb. o veřejných zakázkách. Realizace výběrového řízení proběhla dle regulí zmiňovaného zákona a dle interních metodik zadavatele MHMP.

Po revizi způsobu zadávání veřejných zakázek malého rozsahu v rámci projektu PCMS, byly tyto zakázky v souladu s interními přepisy MHMP a soutěženy mezi 3 subjekty (minimálně), a to v převážné většině prostřednictvím tzv. certifikovaného elektronického tržiště a nad rámec tohoto předpisu je veřejná zakázka zobrazena i na veřejné úřední desce MHMP (praxe od roku 2008).

Po věcné stránce veřejné zakázky malého rozsahu na konzultační služby, na služby řízení projektu a na právní služby, byly zadávány zřejmě v návaznosti na aktuální vývoj projektu PCMS a jeho subprojektů.

Vnímáme však nedostatky v oblasti plánování takto zadávaných služeb. Pro podrobnější informace bude nutná další revize okolností a formy zadání jednotlivých zakázek a dílčích projektů PCMS.

9.1.7. Systémová pochybení v rámci projektu

Na projektu, od jeho samotného počátku (2006), respektive v prvních měsících po zahájení projektu, byla zvolena strategie najmout do projektových týmů, které byly zodpovědné za projektové řízení, externí odborníky třetích stran z důvodu, že MHMP nedisponuje dostatečnou kapacitou odborníků s dostatečnou expertní znalostí a kompetencí. Tato strategie snížila možnou kontrolu projektu ze strany MHMP, současně však také došlo k opakované změně subjektu, který externí odborníky

pro tuto oblast poskytoval a ze strany kompetentních osob byl tento stav podceněn.

Při zkoumání byla získána projektová dokumentace odpovídající standardům vedení projektu zhruba od přelomu roku 2007/2008, podklady před touto dobou se nepodařilo získat v kompletní podobě a je pravděpodobné, že do roku 2007 docházelo k významným pochybením na straně projektového řízení.

Na projektovém řízení, vedoucí projektu, či jako dozor investora se podílely tyto subjekty:

- Soluziona, s.r.o. (následně přejmenována na INDRA Czech Republic, s.r.o.)
- Axcode, s.r.o.
- PADCOM, s.r.o.
- Deloitte Advisory, s.r.o.

Dalším šetřením jsme zjistili, že ze strany MHMP nebyly dodržovány a důsledně vyžadovány v rámci projektu termíny uvedené v harmonogramu a akceptace, hlavně v počáteční části projektu probíhaly bez jakýchkoliv výhrad.

Přesto pokud porovnáme, jakým způsobem projektově pracoval s předávacími protokoly a důslednou evidencí procesování výhrad a jejich odstranění DPP a MHMP, trval DPP velmi důsledně na evidenci jakýchkoliv nedostatků, zatímco MHMP akceptoval předané části systému i přes jeho zjevnou komplikovanost relativně hladce. DPP navíc pravidelně aktualizuje a eviduje případné nesrovnalosti a nekompromisně vyjednává s dodavatelem ohledně komplexního plnění, které zahrnuje dané nedostatky.

MHMP doložil podobná jednání v menším rozsahu u aplikace parkovného, přesto však při srovnání způsobu akceptace považujeme způsob akceptace MHMP jako málo důsledný i přesto, že postupnými kroky dochází od roku 2008 k nápravě tohoto stavu a zvyšuje se důslednost a kompetence jednotlivých kroků.

Naše zkoumání tak potvrzuje významná systémová pochybení v původním nastavení a způsobu vedení projektu, zadávání nových požadavků, projektového řízení a s tím souvisejícím neefektivním vynakládáním prostředků na projekt PCMS v návaznosti na charakter nastavených smluvních a licenčních vztahů.

I přes postupné kroky, zaměřené k nápravě tohoto stavu, se nepodařilo ke 30.6.2009 tento stav dostatečně změnit ve prospěch MHMP. Této problematice jsme věnovali zvýšenou péči v průběhu druhé fáze posuzování projektu PCMS. Je obvyklé, že u obdobných projektů existuje tzv. sponzor projektu, např. - člen rady a nejméně jeden zaměstnanec, který je plně odpovědný za průběh projektu.

Jde zejména o oblasti:

- Nepřiměřené a obtížně kontrolovatelné náklady způsobené přenesením projektového řízení na subjekty třetích stran bez přímé, pravidelné a metodické kontroly.
- Nereálná koncepce související s vynakládáním investičních nákladů ve vztahu k příjmové stránce projektu.
- Nejasná politika v oblasti sekundárních nákladů souvisejících s provozem a údržbou systému/systémů, zejména v oblasti licencování systému a jeho podsystémů způsobného pravděpodobně zhoršenou vyjednávací pozici MHMP.
- Vyvolání sekundárních nákladů u poskytovatele služby DPP (Dopravní podnik Praha), jako například napojení na ERP systém SAP.
- Vyvolání sekundárních nákladů u poskytovatele služby Městské knihovny.

V rámci zkoumání se nám nepodařilo získat dostatek informací, které by prokazovaly, že MHMP předkládal společnosti Haguess testy funkcionality, které musí proběhnout pro akceptaci a tyto testy byly definovány přímo dodavatelem.

9.2. Použité vstupy, informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společnosti Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace s DPP
- Osobní konzultace s odborem legislativy MHMP
- Osobní konzultace s právní kanceláří Randa Legal
- Konzultace Deloitte
- Zákony o veřejných zakázkách a to zákon č.40/2004 Sb. a zákon č.137/2006 Sb.
- Obchodní zákoník
- Metodiky projektového řízení – Best Practices
- Veřejné informační zdroje

10. Bezpečnostní rizika

10.1. Výchozí stav

Karta MIFARE Classic je v podstatě standardizovaná paměťová karta se základními bezpečnostními pravidly pro řízení přístupu. Její paměť je rozdělena do segmentů a bloků. Vzhledem k ceně a odolnosti je tato karta široce rozšířená pro aplikace typu elektronické peněženky, přístupových systémů, elektronických jízdenek nebo vstupenek a dalších identifikačních karetních systémů.

Karta využívaná v první fázi projektu Opencard nabízí 4096 bajtů paměťové kapacity (4kB), rozdělených celkem do 40 sektorů, přičemž každý sektor je chráněn dvěma různými klíči (nazývanými A a B). Tyto klíče mohou mít nastavena práva např. pro čtení, zápis apod. Každá karta má v prvních 16 bytech uloženo jedinečné sériové číslo a další informace o výrobci, která nelze přepisovat jako zbytek paměti. Celkový prostor pro uložení aplikačních dat je tak snížen na 3440 bytů, což je však pro aplikace, jaké Opencard nabízí, případně může nabízet dostatečné. Celosvětově nejznámější podobnou implementací je Londýnská Oyster card.

MIFARE Classic využívá šifru Crypto-1, kterou lze relativně snadno prolomit s pomocí běžného osobního počítače během několika vteřin pokud zná útočník k dispozici 50 bitů klíče. Tento útok dokáže ve speciálních případech odchytit klíč. Existuje více typů útoků, z nichž některé dokáží získat privátní klíč během zlomku vteřiny. Poslední známé útoky se zaměřují na přímý útok na kartu a to opakovanou komunikací s kartou, přesto potřebují několik stovek dotazů, aby privátní klíč získaly. Karty lze za speciálních podmínek i klonovat. Přesto je karta obecně považována za relativně bezpečnou, jelikož při běžném provozu je nutné kartu přiložit ke čtečce na vzdálenost 30-100 mm.

Patrně z tohoto důvodu bylo později přikročeno ke změně používaných karet na MIFARE DESFire, které díky použitému hardwarovému šifrovacímu akcelerátoru, který je podmínkou pro šifrovanou komunikaci v reálném čase, dokážou většině známých útoků snadno odolat a přenášené informace jsou šifrovány, čímž klesá možnost takovou komunikaci odchytit a šifru prolomit. Systémy, které podporují jednu z karet, dokážou technologicky podporovat i druhý typ karty, jelikož pro komunikace používají stejných standardů, frekvencí apod. Z aplikačního pohledu je však způsob každé karty odlišný.

10.1.1. Interní bezpečnostní pravidla společnosti Haguess

Společnost Haguess předložila ke zkoumání i dokumentaci týkající se bezpečnostní politiky, který se zabývá riziky a jejich zhodnocením. Tato pravidla prošla poslední aktualizací k 1.9.2009 a k dispozici jsme získali dokumenty aktuální verze. Zhodnocením rizik se rozumí zejména

specifikace preventivních opatření, scénářů reakce, pokud riziko nastane a specifikace dopadu příslušného rizika. Provozovatel systému SKC dle dokumentace vyhodnocuje rizika pro následující organizační složky SKC:

- Kontaktní místa (přepážky)
- Provozní pracoviště
- Serverovnu
- Externí personalizační linku

Metodika zhodnocení rizik záleží na volbě provozovatele SKC, na jeho dispozici i interní bezpečnostní politice. HMP provedl prostřednictvím třetích stran nejméně jednou ročně (2007 společnosti Relsie, 2008 společnosti Deloitte, 2009 společnost XEOS) prověření bezpečnostních pravidel a analýzy rizik ve firmě Haguess, která následně dokumentaci i postupy aktualizovala. Poslední verze, datovaná, platná a aktualizovaná k 1.9.2009 obsahuje komplexní pokrytí rizik i bezpečnostních politik.

V rámci hodnocení rizik jsou hodnocena následující rizika:

- Chyba zaměstnanců při příjmů podkladů nebo provozu systému
- Krádež či ztráta karet připravených k předání
- Krádež čtečky bezkontaktního čipu karet
- Krádež formulářů žádostí s vyplněnými osobními údaji
- Krádež pokladní zásuvky
- Krádež pracovní stanice
- Krádež tiskárny dokladů
- Napadení systému SKC škodlivým software
- Nedostatečná zpracovatelská kapacita kontaktního místa (úplné vytížení)
- Nedostatek kvalifikovaných zaměstnanců pro provoz kontaktního místa
- Nedostatek kvalifikovaných zaměstnanců pro provozní pracoviště
- Nedostatek kvalifikovaných zaměstnanců pro správu serverového parku
- Neoprávněný přístup do serverovny.
- Neoprávněný přístup na provozní pracoviště
- Neoprávněný vstup do databáze nebo k systémům na serverech s důsledkem ztráty dat nebo systému
- Odposlech dat, útočník odposlechne komunikaci mezi čtečkou a kartou
- Poškození prachem nebo drobnými mechanickými částicemi
- Poškození vedení/kabeláže komunikačního kanálu
- Použití paměťového média (např. Flash disk) pro vyjmutí dat ze systému na PC
- Použití software neautorizovaným způsobem
- Použití zbraní, útočník se pokusí získat hotovost uloženou na přepážce.
- Povodeň
- Požár
- Předstírání identity uživatele, který se chce dostat k systému
- Přetížení komunikačního spojení
- Selhání dodávky energie nebo kolísání napětí v rozvodné síti

- Selhání HW serveru
- Selhání HW, pracovní stanice nebo periferie
- Selhání klimatizace
- Selhání sítě a síťových prvků
- Výpadek komunikačního spojení mezi KM a centrálním pracovištěm
- Zemětřesení

10.2. Posouzení

V době vzniku projektu i v době změny technologie existovaly karty umožňující šifrování pomocí 128 bitové šifry AES, která je z pohledu možnosti napadení bezpečnější, přesto lze označit aktuálně používanou kartu MIFARE DESFire za dostatečně zabezpečenou pro potřeby, ke kterým je karta určena.

V průběhu analýzy jsme prošli bezpečnostní dokumentaci a analýzu rizik a vybrané oblasti jsme prověřili. Z důvodu citlivosti mnoha z těchto informací není možné většinu informací obsažených v této dokumentaci uvádět v tomto dokumentu, jelikož jejich uvedením by mohlo dojít k porušení některého z pravidel. Vzhledem k tomu, že dokumentace byla na základě kroků HMP aktualizována naposledy k 1.9.2009 a následně akceptována a současně vzhledem k tomu, že HMP má kompletní kopii dokumentace k dispozici, konstatujeme, že bezpečnostní dokumentace a analýza rizik odpovídá rozsahem i obsahem obvyklým zvyklostem a splňuje požadavky, které HMP na tuto dokumentaci má.

Klíčová část informací byla zkoumána pouze nahlédnutím a nebyla kopírována ani zapůjčena mimo sídlo společnosti Haguess, aby nemohlo dojít k jejich kompromitaci ani náhodným způsobem (ztráta paměťového zařízení apod.).

I přes tento závěr doporučujeme HMP, aby v této oblasti pokračoval v pravidelné kontrole a současně, aby společnost Haguess požádal o předložení Disaster and Recovery plánu a Business Continuity plánu v aktualizované podobě, jelikož jde o kritické dokumenty pro provoz celého systému Opencard a jejich aktualizace, prověřování a dodržování by mělo být jednou z hlavních činností ze strany HMP.

10.3. Použité vstupy, informační zdroje

- Technologická specifikace karty MIFARE Classic
- Technologická specifikace karty MIFARE DESFire
- Bezpečnostní normy
- Kryptovací algoritmy
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společností Haguess

- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace s DPP
- Osobní konzultace s odborem legislativy MHMP
- Osobní konzultace s právní kanceláří Randa Legal
- Konzultace Deloitte
- Metodiky projektového řízení – Best Practices
- Veřejné informační zdroje

11. Vymezení stěžejních rizik projektu a dalšího rozvoje

11.1. Posouzení

Projekt sám o sobě nese v současné podobě množství rizik.

Nejdůležitějšími z nich jsou:

- Riziko, že celé řešení nebude akceptováno uživateli (Pražany)
- Projektové řízení (2006-2007) probíhalo mimo odbor informatiky MHMP, bylo outsourcováno a současně se při řízení projektu vystřídalo několik společností bez dostatečně definovaných pravidel zodpovědností a jejich předávání/přebírání.
- Velkým rizikem projektu je zatím omezená funkcionalita karty (není multifunkční)
- Oproti původním očekáváním není zprovozněno plánované portfolio kartových aplikací
- Rizikem při zavedení byla dlouhá doba realizace k prvnímu „masovějšímu" rozšíření - roční předplatné MHD
- Významným rizikem pro rozvoj aplikací typu elektronická peněženka je fakt, že pro finanční služby nebyl získán významný finanční partner - banka, tím vzniká přenesený problém chybějící bankovní licence pro elektronickou peněženku a přináší nutnost řešení plateb pomocí výjimek.
- Součinnost DPP (ukončil participaci na projektu březen 2009)
- Rizikem projektu se stal i fakt, že DPP vyhlašoval vlastní výběrová řízení na činnosti související s projektem PCMS bez přímé koordinace s MHMP
- Projektovým rizikem je závislost MHMP na jednom exkluzivním dodavateli (Haguess)
- Při výběrových řízení typu JŘBU - jednací řízení bez uveřejnění, nebyla ověřována obvyklost a přiměřenost sjednané ceny.
- Výchozím rizikem projektu byl i fakt, že dodavatel (Haguess) neměl dle dostupných informací dostatečné reference v dané oblasti. Toto riziko se za dobu existence z technologického hlediska ukázalo jako neopodstatněné, přesto však mohou některé kroky v průběhu projektu souviset i s tímto rizikem
- Obecně jsou velkým rizikem podobných projektů formy bezpečnosti a to jak technické a technologické, tak z pohledu business kontinuity apod. V tuto chvíli existují krizové scénáře v případě „výpadku" systému, ale nebyly plně dopracovány a akceptovány v rámci projektu.
- Rizikem je i neexistence nástroje nebo metodiky řízení rizik, Disaster & Recovery plánu apod. V tuto chvíli existují samostatné dokumenty v určité fázi rozpracovanosti u společnosti Haguess, ale nikde neexistuje podobný plán pro projekt Opencard jako celek, který by zahrnoval všechny zúčastněné subjekty

11.2. Cílový stav

Cílový stavem projektu Opencard by mělo být vybudování identifikačního a platebního, multiaplikačního nástroje pro občany a návštěvníky HMP s podobným nebo ještě lépe vyšším rozsahem, jako je obvykle v moderních evropských i světových metropolích (například Oyster Card v Londýně, nebo Octopus Card v Hong Kongu).

Využití Opencard by mělo být zaměřeno hlavně do následujících oblastí:

- Technologické zázemí – hybridní karta, multiplikační centrum, platební a zúčtovací systém, elektronická peněženka – tzv. mikroplatby (mikropayment)
- Městské služby – knihovny, kultura, sport, školství
- Turistické aplikace – jednotlivé jízdné (SMS jízdenky fungují jen pro klienty českých operátorů), denní, trojdenní, týdenní, parkování, kultura, sport, služby, ubytování, ...
- Konferenční, kongresová a veletržní aplikace – identifikační karta, které slouží současně pro pobyt ve městě
- Dopravní infrastruktura – parkovací zóny, MHD, krátkodobé jízdné, mýtný systém, ...
- Městské utility – elektřina, voda, plyn, teplo, odpady
- Městské kontaktní centrum – portál města, přepážkový systém, terminály, čtečky, call centrum, městská policie
- Zdravotnictví – nemocnice, polikliniky, záchranná služba, sociální služby, soukromé ordinace, ...
- Komerční organizace – obchodní řetězce, restaurace, hotely, stravování pro zaměstnance, internet platby, benzínová čerpadla, prodejní automaty (káva, nápoje, občerstvení), kina, taxi, ...

11.3. Použité vstupy, informační zdroje

- Zadávací dokumentace v rámci výběrového řízení „Realizace servisního kartového centra"
- Nabídkový dokument společnosti Haguess na realizaci díla
- Smlouvy, včetně jejich dodatků
- Technická data a dokumenty poskytnuté odborem informatiky MHMP
- Osobní konzultace s odborem informatiky MHMP
- Dokumentace poskytnutá společností Haguess
- Osobní konzultace se společností Haguess
- Technická data a dokumenty poskytnuté DPP
- Osobní konzultace DPP
- Osobní konzultace s odborem legislativy MHMP
- Osobní konzultace s právní kanceláří Randa Legal
- Konzultace Deloitte
- Zákony o veřejných zakázkách a to zákona č.40/2004 Sb. a zákona č.137/2006 Sb.
- Obchodní zákoník
- Metodiky projektového řízení – Best Practices
- Veřejné informační zdroje

12. Doporučení pro další technologický rozvoj

Technologicky považujeme projekt Opencard za progresivní a dlouhodobě udržitelný projekt, přesto je nutné pracovat s trendy, které v dané oblasti ovlivňují další rozvoj podobných systémů.

12.1. Výchozí stav

Projekt Opencard vychází ze standardizovaných vysokofrekvenčních bezdrátových technologických řešení, jakými jsou MIFARE Classic (Standard), později v projektu nahrazeného MIFARE DESFire, který využívá podobné technologie jako původní čip MIFARE Classic, ale na rozdíl od něj je rozšířen o další hardwarové a softwarové funkce a obsahuje DESFire operační systém, který nabízí jednoduchou adresářovou strukturu se soubory, které jsou typicky používány u SMART karet. Toto řešení respektuje současné trendy v této oblasti a je jedním z preferovaných řešení. Díky standardu MIFARE DESFire je vytvořena bezpečná a flexibilní platforma pro nejširší použití aplikací na bázi bezkontaktního čipu, kam patří dopravní aplikace, turistické aplikace, elektronická peněženka apod.

12.2. Posouzení

Klíčovým prvkem současného stavu projektu Opencard je existující kmen 385 000 vydaných karet. Z tohoto pohledu lze považovat zvolenou strategii, která byla založena na masivním rozšíření počtu uživatelů pomocí aplikace elektronických předplatných kupónu na městskou hromadnou dopravu, za jednu z možných. Pokud se podíváme na celkový potenciál dopravní aplikace, je reálné existující kmen rozšířit na 660 000 vydaných a používaných karet. Důležité však je neopakovat stav, kdy z 385 000 vydaných karet, které mají nahranou dopravní aplikaci, obsahuje pouze 260 000 karet některý z časových kupónů a zbývající karty nejsou z pohledu dopravní aplikace používány.

Pokud MHMP plánuje masivní rozšíření karet za současného rozšíření aplikací i do jiných oblastí, aby se karta stala skutečně multifunkčním nástrojem a vynikly tak veškeré výhody jak technologie, tak projektu, je nutné naplánovat takový způsob zavádění, aby pro občana bylo jednoznačně výhodné Opencard používat.

V současnosti existuje větší množství úspěšných "městských" karet založených na kmenu uživatelů dopravních aplikací, z kterých se dají převzít pozitivní a rychle implementovatelné funkcionality a současně se lze vyvarovat dalších možných obchodně organizačních chyb, které by projekt v očích uživatelů poškodily.

Pokud má být použití Opencard v dopravě úspěšné, je nutné podpořit co nejširší škálu možných funkcí a případně i přizpůsobit některé produkty potřebám, které vzniknou až zavedením elektronických kupónů Opencard. Zavedení jednotlivého jízdného se z pohledu investiční náročnosti, kterou pro DPP ve své analýze vyčíslila společnost Deloitte na 340 milionů Kč, zdá nerealizovatelná, přesto doporučujeme tuto variantu předem nezavrhovat, jelikož funguje v mnoha světových metropolích již několik let a je hodnocena pozitivně jak uživateli, tak v konečném důsledku i poskytovateli dopravních služeb, jelikož vychází z obecně platného standard karetu MIFARE a pokud jsou touto cestou distribuovány předplatní kupóny v různé délce předplatného, je vysoce pravděpodobné, že jednotný standard pro všechny typy jízdného by přinesl pozitivní efekt i přesto, že pro jednotlivé jízdné existují další alternativní kanály.

Co nejširší využívání dopravní aplikace považujeme za klíčový prvek pro masivní rozšíření a využívání Opencard, což je podmínka pro co nejvýhodnější vyjednávací pozici HMP se strategickým partnerem, který je nezbytný pro zavedení elektronické peněženky.

12.2.1. Budoucí technologie NFC

Možným nástupcem nebo doplňkem technologií vysokofrekvenčních bezkontaktních karet je technologie, která se stává standardem pro mobilní telefony s názvem NFC – Near Field Communication (komunikace blízkého pole, nebo spíše komunikace na velmi krátkou vzdálenost (obvykle do 100 mm). V rámci technologie NFC je na trhu několik pilotních projektů a v nabídce několik modelů nejméně od 6 výrobců:

- Benq T80
- LG 600V contactless
- Motorola L7 (SLVR)
- Nokia 3220 + NFC Shell
- Nokia 6131
- Nokia 6216 Classic
- Nokia 6212 Classic
- SAGEM my700X Contactless
- Samsung SGH-X700 NFC
- Samsung D500E

Vzhledem k rychlosti obměny modelů mobilních telefonů u výrobce a vzhledem k rychlosti výměny mobilních přístrojů ze strany uživatelů lze předpokládat, že během 2-3 let může docházet k masivnějšímu nasazení telefonů vybavených technologií NFC na trhu. Proto je potřebné připravit strategii pro jednání s mobilními operátory, která by vedla k přípravě pilotního projektu a hlavně by zajistila pokračování projektu Opencard a jím vybudovaných služeb s využitím vyjednávací pozice a infrastruktury.

Současně doporučujeme, aby budovaná infrastruktura zohledňovala tento budoucí vývoj a neomezovala se pouze na stávající technologie použité v projektu. Při zohlednění budoucích standardů dojde jednoznačně

k úspoře nákladů na implementaci nových technologií (historicky lze v rámci projektu demonstrovat na přechodu ze standardu MIFARE Classic na MIFARE DESFire) a současně dojde k rychlejší integraci nových prvků systému do projektu Opencard.

12.3. Použité vstupy, informační zdroje

- http://europe.nokia.com/find-products/devices/nokia-6216-classic/specifications
- http://europe.nokia.com/A4991361
- http://www.gsmworld.com/documents/gsma_pbm_white_paper_11_2007.pdf
- http://www.nfc-research.at/index.php?id=45
- http://mobilementalism.com/2006/02/11/samsung-and-philips-to-show-off-prototype-nfc-phone-at-3gsm/
- Veřejné informační zdroje

13. Použité zkratky v dokumentu

Zkratka	Popis
PCMS	Prague Card Management Systém
OC	Opencard
SKC	Servisní kartové centrum
DOS	Dopravní odbavovací systém
KAP	Kartová aplikace parkování
PCKS	Pražské centrum kartových služeb
HMP	Hlavní město Praha
MHMP	Magistrát hlavního města Prahy
HGS	Haguess
DPP	Dopravní podnik hlavního města Prahy
MHD	Městská hromadná doprava
JŘBU	Jednací řízení bez uveřejnění
NFC	Near Field Communication (komunikace blízkého pole, nebo spíše komunikace na velmi krátkou vzdálenost (obvykle do 100 mm)"
RFID	Radio Frequency IDentification – radiofrekvenční identifikace

Ing. Jiří Berger - znalec
Číslo dle znaleckého deníku 208/106/2009

V Praze dne 8. ledna 2010

Výtisk číslo: 1
Počet listů: 4

Magistrát hlavního města Prahy
Mariánské náměstí 2
110 00 Praha 1

ZNALECKÝ POSUDEK

z oboru kybernetika
odvětví výpočetní technika

Já, níže podepsaný, Ing. Jiří Berger, bytem Hálkova 181, Veltrusy, 277 46, okres Mělník, jako znalec specializovaný na znaleckou činnost v oboru Kybernetika – výpočetní technika, specializace Výpočetní a komunikační technika, bezpečnost informačních systémů vydávám tento

Znalecký posudek

na základě zpracování projektu: „Technologické posouzení infrastruktury PCMS" pro zadavatele Magistrát hlavního města Prahy jsem byl požádán o zpracování posudku zaměřeného na bezpečnost karetních technologií, použitých v projektu. Tento posudek je součástí kompletního posouzení společnosti e-FRACTAL, jako samostatná část.

Znalci doručeno dne 30. listopadu 2009.

1. ÚVOD

1.1 Popis:

V rámci projektu „Technologické posouzení infrastruktury PCMS" pro zadavatele Magistrát hlavního města Prahy je jako integrální část posouzení potřebné posouzení použitých karetních technologií z pohledu bezpečnosti. Na zahájení projektu byla zvolena hybridní karta s bezkontaktním čipem standardu MIFARE Classic, později v průběhu projektu byla tato technologie nahrazena technologií MIFARE DESFire. Cílem posouzení je posouzení obou těchto technologií, rozdílů mezi nimi a zhodnocení jejich bezpečnosti.

Pro potřebu znaleckého posudku byla předložena projektová dokumentace jak ze strany Magistrátu hlavního města a společnosti Haguess. Současně mi bylo umožněno dle potřeby nahlédnout do dalších dokumentů, které svým charakterem nemohly být z důvodu dodržení bezpečnostních pravidel předány ani kopírovány pro mé zkoumání.
Při zpracování jsem dále vycházel z veřejně dostupných dokumentů, z dokumentů, které mi byly předloženy jako podklady související s projektem.

1.2. Otázky, které mají být zodpovězeny:

Porovnejte karetní technologie MIFARE Classic a MIFARE DESFire a zhodnoťte jejich bezpečnost z pohledu použití v rámci projektu Opencard.

2. NÁLEZ

2.1. Historie karet MIFARE

Čip MIFARE byl vyvinut společností Mikron, která se v roce 1998 díky akvizici stala součástí společnosti Philips.
V roce 1994 byla poprvé představena technologie MIFARE Classic 1k a o dva roky později, v roce 1996 byla představena na bázi této karty první aplikace v oblasti dopravy v jihokorejském Soulu. V dalších letech proběhlo několik úprav a vylepšení směřujících k zajištění vyššího stupně bezpečnosti. V roce 1997 to byl čip MIFARE PRO který obsahoval koprocesor, v roce 1999 byl představen čip MIFARE PROX který měl koprocesor podporující privátní klíče.
Zásadní změnu přinesl rok 2002, kdy byla představena zcela nová řada čipů MIFARE DESFire, která již nebyla pouhým paměťovým médiem, ale obsahovala vlastní procesor. Její plné nasazení proběhlo v roce 2004, kdy byly zahájeny činnosti na prvních dopravních aplikacích, využívajících tento čip. Tyto aplikace byly komerčně nasazeny v letech 2005-2006.
Vývoj však pokračoval dál a postupně byly představeny další karty: v roce 2006 to byla karta s čipem MIFARE DESFire EV1, která jako první podporovala šifrování dle standardu 128-bit AES, v roce 2008 byla představena náhrada za kartu MIFARE Classic pod názvem MIFARE Plus a také nabídla šifru 128-bit AES.

2.2. Popis karet s bezkontaktními čipy MIFARE Classic

Bezkontaktní čipy technologického standardu MIFARE představují celosvětově zdaleka nejrozšířenější čipy dodávané mnoha výrobci. Jejich nejčastějším použitím jsou aplikace elektronické peněženky, řešení přístupových systémů, firemní identifikační řešení nebo lístky či kupóny na dopravní řešení, sportovní a kulturní akce. Karty s bezkontaktním čipem MIFARE Standard 4kB nabízejí vyváženou úroveň bezpečnosti (Šifrovaný bezkontaktní přístup (čtení i zápis) k jednotlivým sektorům je zabezpečen dvěma různými klíči a u každého klíče lze nadefinovat povolené operace s daty v jednotlivých blocích. Je použita třístupňová autentizace je mezi kartou a čtečkou pro přístup k datům do jednotlivých sektorů dle ISO normy (ISO 9798-2).

Mezi hlavní parametry patří šifrování přenášených dat s ochranou proti zneužití odposlechnutých autentizací dat karty jejich zopakováním při podvodné autentizaci. Samostatný pár klíčů pro každý ze 40 sektorů umožňuje provozovat velký počet nezávislých aplikací, kdy data jedné z nich nejsou přístupná ostatním. Karta MIFARE Standard je v souladu s normou ISO 14443 definující bezkontaktní interface. Díky širokému rozšíření existuje velké množství ověřených kartových aplikací. Karty s čipem MIFARE Standard jsou kompatibilní se čtecími zařízeními pro MIFARE DESFire. V obecné rovině lze říci, že karta s čipem MIFARE Classic má nižší cenu než karta s čipem MIFARE DESFire
Karta s čipem MIFARE Classic odpovídá standardu Mifare Application Directory (MAD1,2), který umožňuje na kartě dynamické rozmístění jedné nebo více aplikací.

Obecně je karta s čipem MIFARE Classic v podstatě jen paměťové médium, které má paměť rozdělenou do segmentů a bloků s jednoduchým bezpečnostním mechanismem, který zajišťuje přístupová práva.
Základní karta MIFARE Classic 1K obsahuje 1024 bajtů pro ukládání dat, která jsou rozdělena do 16 sektorů, přičemž každý sektor je chráněn dvěma rozdílnými klíči, označovanými A a B. Každý z nich může mít naprogramovanou funkci přístupu k zvolenému sektoru jako je například čtení, zápis, zvýšení hodnoty apod. Novější a více rozšířená karta s čipem MIFARE Classic 4K, který byla použita i v pilotním provozu Opencard již nabízí 4096 bajtů, rozdělených do celkem čtyřiceti sektorů, z nichž 32 má stejnou velikost jako na původní základní kartě s čipem MIFARE Classic 1K a dále má osm dalších sektorů o čtyřnásobné velikosti oproti základní 1K verzi. Kromě těchto dvou typů existuje ještě karta s čipem MIFARE Classic mini, která však nabízí pouze 320 bajtů rozdělených do pěti sektorů.
Na všech těchto kartách je pro každý sektor rezervováno 16 bajtů pro uložení klíčů a přístupových práv a nelze je za běžných podmínek použít pro uživatelská data. Současně prvních 16 bajtů

paměťového prostoru každé karty obsahuje unikátní sériové číslo karty společně s identifikací výrobce, které nelze měnit. Po odečtení těchto pevně definovaných datových položek je čistá úložná kapacita 752 bajtů pro čip MIFARE Classic 1K, 3440 bajtů pro Classic 4K a 224 bajtů pro Mini.

2.3. Bezpečnost karty s čipem MIFARE Classic

Karty s bezdrátovým čipem MIFARE Classic používají šifrovací algoritmus Crypto-1. Vzhledem k současnému stavu technologií lze šifru prolomit v řádu deseti vteřin s pomocí přenosného počítače, pokud zná útočník pouhých 50 bitů veřejného klíče. Takový útok je založen na klíči získaného podvrženou transakcí za určitých okolností. Podrobné postupy byly opakovaně publikovány na akademické půdě nebo na různých konferencích.

Dalším možným známým útokem je možnost získat pomocí přenosného počítače privátní klíč během několika desítek milisekund za předpokladu, že je získán přístup k oprávněné čtečce.

Existuje ještě množství dalších útoků, které pracují napřímo s čipem na kartě bude platného čtecího zařízení. Speciálně v posledním roce (2009) bylo publikováno množství úroků, které umožňují relativně velmi rychlý přístup k získání klíčů. Patrně nejvážnější hrozbou pro tuto technologii je typ útoku, který dokáže během cca 10 sekund vyrobit klon původní karty.

2.4. Popis karet s bezkontaktním z čipem MIFARE DESFire

Karta s čipem MIFARE DESFire je založena na mikroprocesorové platformě, která historicky vychází z řešení, jakými bylo například MIFARE ProX/SmartMX. Na rozdíl od nich však obsahuje daleko vyšší úroveň bezpečnostních vlastností, které jsou jak hardwarové, tak softwarové. Na rozdíl od MIFARE Classic obsahuje kromě mikroprocesoru také operační systém (DESFire OS) a paměť není rozdělena do pevných segmentů, ale naopak obsahuje adresářovou strukturu, podobou, jaká se dnes používá na tzv. smart kartách (SIM karty sítě GSM, platební karty s čipem apod.). Takto navržená struktura přináší flexibilní možnosti rozdělení paměti a je navíc podpořena vysokou transakční rychlostí. Karty jsou nabízeny v několika variantách a to varianta s Triple-DES šifrou a několik variant s AES šifrou, kdy varianty se liší velikostí úložného prostoru (2,4 a 8 KB). Karta je založena na procesoru 8051 s koprocesorem optimalizovaným na rychlý výpočet 3DES, respektive AES šifrovacího algoritmu.
Název karty DESFire je odvozen právě od 3DES algoritmu. Druhá část názvu je v podstatě obchodním tahem, jelikož slovo F i r e se skládá z prvních písmen klíčových marketingových a prodejních vlastností produktu: Fast (rychlý), Innovative (inovativní, progresivní), Reliable (spolehlivý) a sEcure (bezpečný).

Specifikace MIFARE DESFire

- MIFARE technologie využívá RF komunikačního kanálu pro spojení se čtečkou
- Přenosový kmitočet 13,56 MHz
- Plná kompatibilita komunikačního kanálu se standardem ISO 14443 (Typ A)
- Podpora antikolizního systému
- Vzdálenost karta – čtečka 0-10 cm
- Rychlý přenos dat oběma směry (až 424 kbit/s)
- Kryptografická podpora algoritmu 3 DES (Triple DES)
- 4 KB paměti EEPROM (zálohovaná paměť čipu pro aplikace)
- Multiaplikační podpora

2.5. Bezpečnost karty s čipem MIFARE DESFire

Bezkontaktní karty vybavené čipem MIFARE DESFire jsou dnes považovány za standard v oblasti poskytování **bezpečných bezkontaktních služeb.** Díky tomu, že je karta s čipem MIFARE DESFire procesorová karta splňující normu ISO 14443 a její interní logická organizace dat a použité komunikační protokoly navazují na standardy ISO, lze je označit za ideální nástroj pro bezkontaktní

transakce. Karta je navržena tak, aby umožňovala multiaplikační využití karty s kompatibilitou více uživatelů.
Klíčovým prvkem karty je bezpečnost, který je na rozdíl od karty MIFARE Classic, jež používala proprietální systém Crypt 1, založena na standardní šifře 3DES a tím je podstatně odolnější proti prolomení. Kromě vlastního výpočetního výkonu, souborového systému a využitému způsobu šifrování má karta také zvýšenou odolnost proti fyzickým útokům (za použití leptání, chladu, tepla, mikrosondy, frekvence hodin aj).

2.6. Shrnutí

Karta MIFIRE Classic představovala ve své době revoluční krok v oblasti bezkontaktnich čipů. Principiálně se jednalo o paměťové médium, a proto bylo s postupem času představeno několik útoků, které umožňují prolomení nebo ohrožení bezpečnosti dat a dokonce klonování karty. I v tomto kontextu je však nutné zhodnotit k jakému účelu je karta používána a zda riziko a náklady nutně vynaložené na prolomení nebo ohrožení bezpečnosti jsou ekvivalentní potenciálnímu užitku. Z pohledu Opencard technologicky považuji kartu MIFARE Classic za jednu z možných variant pro pilotní projekt, plně se však ztotožňuji s rozhodnutím nevyužít tento typ karty pro běžný provoz. Naopak volbu karty s bezkontaktním čipem MIFARE DESFire považuji za správnou a perspektivní i z pohledu dalšího rozvoje projektu Opencard a s ním souvisejících aplikací. Bezpečnostní hledisko, které je u takto rozsáhlých projektů a hlavně u projektů, které pracují s finančními prostředky (ať již platba parkovného, nebo další plánované aplikace) jedním z klíčových parametrů, je u karty MIFIRE DESFire na velmi vysoké úrovni a to jak z pohledu ochrany dat uložených na vlastní kartě, tak z pohledu možnosti „odposlechu" dat. Kartu s bezkontaktním čipem MIFARE DESFire považuji za správnou volbu pro projekt Opencard.

Z pohledu uživatele lze identifikovat dvě zásadní výhody karty MIFARE DESFire proti kartě MIFARE Standard ve výrazně vyšší bezpečnosti karetního systému a možnosti skutečného multiaplikačního a multiuživatelského využití.

3. ZÁVĚR

Na základě provedeného zkoumání vydávám toto posouzení:

Otázka: Porovnejte karetní technologie MIFARE Classic a MIFARE DESFire a zhodnoťte jejich bezpečnost z pohledu použití v rámci projektu Opencard.

Odpověď: Z pohledu projektu Opencard technologicky považuji kartu MIFARE Classic za jednu z možných variant pro pilotní projekt, plně se však ztotožňuji s rozhodnutím **nevyužít** tento typ karty pro běžný provoz. Naopak volbu karty s bezkontaktním čipem MIFARE DESFire **považuji za správnou a perspektivní** i z pohledu dalšího rozvoje projektu Opencard a s ním souvisejících aplikací.

Znalecký posudek jsem podal jako znalec, jmenovaný rozhodnutím Krajského soudu v Praze ze dne 20.6.2007 č.j. Spr. 4127/2005 pro základní obor kybernetika, pro odvětví výpočetní technika se specializací výpočetní a komunikační technika, bezpečnost informačních systémů.
Znalecký úkon je zapsán pod pořadovým číslem 208/106/2009 znaleckého deníku.

Znalecký posudek zpracoval:
znalec v oboru kybernetika
odvětví výpočetní technika
Ing. Jiří Berger