

Smlouva o dílo

I. SMLUVNÍ STRANY

1. Objednatel

Kraj Vysočina

zastoupený: Ing. Miroslavem Houškou, náměstkem hejtmana
se sídlem: Žižkova 57, 586 01 Jihlava
IČO: 70890749
bankovní spojení (číslo účtu): 123-6403810267/0100
123-6403610257/0100
123-6404210247/0100
e-mail: posta@kr-vysocina.cz
tel.: 564 602 111
ID datové schránky: ksab3eu
kontaktní osoba ve věcech technických: Ing. Václav Zikán, vedoucí oddělení dopravní
obslužnosti, tel.: +420 564 602 178, e-mail: zikan.v@kr-vysocina.cz

(dále jen „**Objednatel**“)

a

2. Zhotovitel

XT-Card a.s.

zastoupený: Ing. Martinem Rejzlem, předsedou představenstva a
Mgr. Lukaszem Sebastianem Kryńským,
místopředsedou představenstva
se sídlem: Seifertova 327/85, 130 00 Praha 3
IČO: 27408256
DIČ: CZ27408256
zapsán v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. B 10398
bankovní spojení (číslo účtu):
e-mail:
tel.:
ID datové schránky:
kontaktní osoba ve věcech technických:

(dále jen „**Zhotovitel**“)

(Objednatel a Zhotovitel společně dále také jako „**Smluvní strany**“)

uzavřeli v souladu s § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“) tuto smlouvu na zhotovení, dodávku a implementaci informačního systému a technologie elektrického odbavení cestujících v integrovaném dopravním systému Veřejné dopravy Vysočiny včetně poskytnutí souvisejících činností (dále jen „**Smlouva o dílo**“ nebo „**Smlouva**“).

II. ÚVODNÍ UJEDNÁNÍ

3. Smlouva o dílo je uzavřena na základě výsledků zadávacího řízení (dále jen „**Řízení Veřejné zakázky**“) nadlimitní veřejné zakázky s názvem **Elektronické odbavení cestujících VDV**, ev. č. zakázky ve Věstníku veřejných zakázek: **Z2022-011525**, sp. zn. zadavatele: **KVEOC0819** (dále jen „**Veřejná zakázka**“). Jednotlivá ujednání Smlouvy o dílo tak budou vykládána v souladu s podmínkami Veřejné zakázky a nabídkou Zhotovitele podanou do Řízení Veřejné zakázky. Současně se Smlouvou je na základě Řízení veřejné zakázky uzavírána také servisní smlouva (dále jen „**Servisní smlouva**“).
4. Účelem Smlouvy o dílo je zajištění fungování systému elektronického odbavení cestujících v integrovaném dopravním systému Veřejné dopravy Vysočiny, a to v souladu se všemi podmínkami sjednanými Smlouvou o dílo.

III. PŘEDMĚT SMLOUVY

5. Zhotovitel se touto Smlouvou zavazuje provést pro Objednatele dílo, které spočívá ve zhotovení, implementaci a dodání informačního systému a technologie elektronického odbavení cestujících (dále jen „**EOC**“) v prostorách Objednatele, včetně zaškolení odborných pracovníků Objednatele pro řádné užívání a údržbu technologie EOC a softwaru EOC (dále jen „**Dílo**“). Přesná specifikace Díla je uvedena ve specifikaci Díla (Příloha č. 1 Smlouvy, dále jen „**Specifikace díla**“).
6. Objednatel se zavazuje zaplatit Zhotoviteli dohodnutou cenu za řádně a včas provedené Dílo, a to za podmínek Smlouvou dále stanovených.
7. Zhotovitel se zavazuje na plnění dle Smlouvy alokovat pracovní kapacitu osob realizačního týmu uvedených v seznamu členů realizačního týmu (Příloha č. 4 Smlouvy, dále jen „**Seznam členů realizačního týmu**“) a k plnění dle Smlouvy využít výhradně těchto osob. Jakákoliv dodatečná změna osoby realizačního týmu musí být předem písemně schválena Objednatelem. Zhotovitel se v takovém případě zavazuje nahradit osobu realizačního týmu takovou osobou, která disponuje požadovanými minimálními znalostmi a odbornou kvalifikací dle požadavků Objednatele uvedených v zadávací dokumentaci Veřejné zakázky a která by v rámci hodnocení nabídek v Řízení Veřejné zakázky neobdržela méně bodů, než obdržela původní osoba realizačního týmu.
8. Zhotovitel se zavazuje provádět Dílo sám, nebo s využitím poddodavatelů uvedených v seznamu poddodavatelů (Příloha č. 3 Smlouvy, dále jen „**Seznam poddodavatelů**“). Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu plnění svěřeného poddodavateli musí být předem písemně schválena Objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval Zhotovitel sám. Smluvní strany výslovně uvádějí, že při provádění Díla prostřednictvím jakékoliv třetí osoby dle tohoto odstavce má Zhotovitel odpovědnost, jako by Dílo prováděl sám.

IV. DOBA A MÍSTO PLNĚNÍ

9. Zhotovitel se Smlouvou zavazuje provést pro Objednatele Dílo do 13 měsíců ode dne účinnosti Smlouvy. Dílo je provedeno, je-li dokončeno, předáno a Objednatelem akceptováno.
10. Předpokládaný harmonogram plnění včetně stanovení hlavních milníků je uveden ve Specifikaci díla. Zhotovitel je povinen dodržovat podrobný harmonogram plnění, který zpracuje v rámci cílového konceptu řešení (prováděcího projektu) ve smyslu Specifikace díla a který musí být

v souladu s předpokládaným harmonogramem dle Specifikace díla. Podrobný harmonogram plnění bude obsahovat termíny plnění pro předání dílčích částí Díla.

11. Místem plnění je sídlo Objednatele, případně jiné místo určené Objednatelem.
12. Pokud to povaha plnění Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Zhotovitel oprávněn provádět části Díla také vzdáleným přístupem.

V. DALŠÍ PRÁVA A POVINNOSTI ZHOTOVITELE

13. Zjistí-li Zhotovitel při provádění Díla skryté překážky a tyto překážky znemožní provedení Díla dohodnutým způsobem, je Zhotovitel povinen oznámit to bez zbytečného odkladu Objednateli a navrhnout změnu Díla.
14. Zhotovitel je povinen upozornit Objednatele na nevhodnost věcí převzatých od Objednatele nebo pokynů daných mu Objednatelem. Pokud nevhodné pokyny brání Zhotoviteli v řádném provádění Díla, je oprávněn přerušit provádění Díla, přičemž o dobu, o kterou bylo nutné přerušit provádění Díla, se na základě dohody Smluvních stran smí prodloužit termín provedení Díla uvedený v odstavci 9 smlouvy.
15. Jestliže Zhotovitel splnil svou povinnost podle odstavce 14 Smlouvy, neodpovídá za nemožnost dokončení Díla nebo za vady dokončeného Díla způsobené nevhodnými pokyny Objednatele.
16. Zhotovitel se zavazuje dodržovat opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele, která jsou specifikována v příloze Smlouvy (Příloha č. 5 Smlouvy, dále jen „**Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatel**“).
17. Zhotovitel je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto Smlouvou ve stejné míře u všech případných poddodavatelů či jiných osob, které mají přístup k informačním aktivům Objednatele prostřednictvím Zhotovitele.
18. Zhotovitel se zavazuje nepoužít Objednatelem poskytnuté dokumenty, data, informace či věci nezbytné pro provedení Díla a informace, které Objednatel nebo jím zřizované a zakládané organizace vloží do EOC za jiným účelem než za účelem splnění této nebo Servisní smlouvy. Zhotovitel není oprávněn využít takto poskytnuté dokumenty, data, informace či věci ke své podnikatelské činnosti ani je zpřístupnit třetím osobám bez souhlasu Objednatele.
19. Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které mu byly v souvislosti se Smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Zhotovitel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Zhotovitele veřejně přístupnými stanou (dále jen „**důvěrné informace**“). Zhotovitel nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele. Povinnosti dle tohoto odstavce je Zhotovitel povinen zachovávat i po zániku této Smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění Zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Zhotovitel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené Zhotoviteli právním předpisem nebo rozhodnutím orgánu veřejné moci.

VI. DALŠÍ PRÁVA A POVINNOSTI OBJEDNATELE

20. Objednatel je povinen na vyžádání Zhotovitele, v přiměřené lhůtě a na své náklady zajistit při provádění Díla konzultace ze strany svých odborných pracovníků, pokud je to pro provádění Díla nezbytné. V případě nesplnění této povinnosti ze strany Objednatele neodpovídá Zhotovitel za případnou škodu ani za případné vady Díla způsobené nesouladem Díla se softwarovým nebo hardwarovým prostředím Objednatele, pokud na tento nesoulad Zhotovitel Objednatele předem upozornil.
21. Objednatel je oprávněn průběžně kontrolovat provádění Díla. Termín provedení kontroly oznámí Objednatel Zhotoviteli nejméně jeden pracovní den před plánovaným provedením kontroly. Zhotovitel může požádat o změnu termínu kontroly, pokud není z technických důvodů možné kontrolu provést v požadovaném termínu.
22. Objednatel je povinen na základě písemné žádosti Zhotovitele předat Zhotoviteli veškeré věci a informace, které jsou nezbytné k provedení Díla a u kterých lze oprávněně předpokládat, že je má Objednatel k dispozici nebo je schopen je opatřit a které z povahy věci není povinen opatřit pro zhotovení Díla Zhotovitel, a to ve lhůtě 5 pracovních dní ode dne doručení žádosti Objednateli. Pokud Objednatel sdělí Zhotoviteli, že není takto požadované věci nebo informace schopen opatřit, nebo je není schopen opatřit ve stanovené lhůtě, jsou Smluvní strany povinny vyvolat jednání směřující k nalezení řešení. Veškeré podkladové materiály, nutné pro provedení Díla, budou Objednatelem předávány Zhotoviteli primárně v elektronické podobě. Jestliže bude Objednatel v prodlení se splněním své povinnosti předat Zhotoviteli věci nebo informace podle tohoto odstavce Smlouvy po dobu delší než 3 měsíce, je Zhotovitel oprávněn od Smlouvy odstoupit písemným oznámením doručeným Objednateli. Zhotovitel má v takovém případě právo na část ceny Díla, která byla v souladu se Smlouvou řádně splněna do doby odstoupení a která je schopna přiměřeně plnit účel dle Smlouvy.
23. Jestliže je pro řádné vytvoření Díla podle Smlouvy na straně Objednatele zapotřebí součinnosti třetí osoby nebo je součástí Díla integrace softwarového či jiného obdobného produktu třetí osoby, který je již aktuálně instalován v prostředí Objednatele, do tohoto Díla, je Objednatel povinen na své náklady zajistit součinnost takové třetí osoby v přiměřených termínech a rozsahu.
24. Objednatel bere na vědomí, že jeho prodlení se splněním povinnosti podle odstavce 20 nebo 22 Smlouvy nebo prodlení třetí osoby s poskytnutím součinnosti v požadovaném rozsahu podle odstavce 23 Smlouvy může mít vliv na plnění termínu provedení Díla podle odstavce 9 Smlouvy. Jestliže se dostane Objednatel do prodlení se splněním povinnosti podle odstavce 20 nebo 22 této Smlouvy nebo do prodlení třetí osoby s poskytnutím součinnosti v požadovaném rozsahu podle odstavce 23 Smlouvy, o stejnou dobu prodlení se na základě dohody Smluvních stran smí prodloužit termín provedení Díla uvedený v odstavci 9 Smlouvy.
25. Objednatel nesmí používat Dílo a další služby Zhotovitele poskytnuté na základě Smlouvy anebo nechat používat Dílo či služby Zhotovitele poskytnuté na základě Smlouvy jakoukoliv třetí osobou v rozporu se zákonem nebo s dobrými mravy. Výjimkou jsou organizace zřizované nebo zakládané Objednatelem či dodavatelé zajišťující nezbytné služby, kterým Objednatel poskytne podlicenci k užití Díla na základě licenčních podmínek Smlouvy. Použití jakéhokoliv materiálu porušujícího právní předpisy je zakázáno. Toto zahrnuje zejména materiály chráněné proti kopírování nebo materiály chráněné výrobním tajemstvím.
26. Objednatel prohlašuje a zaručuje, že na všechny věci související s vytvořením Díla předávané Zhotoviteli disponuje veškerými potřebnými právy z hlediska autorských práv a zejména zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) (dále jen „autorský zákon“), anebo disponuje příslušnými

licencemi opravňujícími Objednatele k užití těchto věcí. Dále Objednatel prohlašuje a zaručuje, že u těch věcí, kde si to jejich charakter žádá, disponuje licenčními oprávněními ke změnám těchto věcí.

27. Objednatel se zavazuje řádně a v souladu se Smlouvou zhotovené Dílo od Zhotovitele převzít a zaplatit za něj dohodnutou odměnu.
28. Objednatel si vyhrazuje právo na provedení kontroly či auditu plnění bezpečnostních požadavků a podmínek stanovených v Požadavcích a opatřeních pro zajištění bezpečnosti informací a informačních aktiv objednatel.
29. V rámci kontroly či auditu dle předchozího odstavce Smlouvy u Zhotovitele se Zhotovitel zavazuje poskytnout Objednateli důkaz o plnění objednatel vybraného požadavku, a to buď fyzicky přímo v provozovně Zhotovitele nebo vzdáleně pomocí elektronických prostředků.
30. Objednatel si vyhrazuje právo na informace o:
 - a. významné změně ovládání Zhotovitele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů (dále jen „ZOK“),
 - b. změně vlastnictví zásadních aktiv Zhotovitele, které souvisejí s plněním Smlouvy,
 - c. změně oprávnění nakládat s těmito aktivy,
 - d. způsobu řízení rizik informační bezpečnosti na straně Zhotovitele.

VII. SOUČINNOST A VZÁJEMNÁ SPOLUPRÁCE

31. Zhotovitel a Objednatel se zavazují ke vzájemné spolupráci za účelem plnění Smlouvy.
32. Objednatel umožní, po dohodě se Zhotovitelem, pro plnění Smlouvy v prostorách Objednatel vhodné podmínky, zejména:
 - a. zajištění přístupu pověřeným osobám Zhotovitele do prostor potřebných pro plnění předmětu Smlouvy;
 - b. poskytnutí informací nezbytně nutných pro splnění předmětu Smlouvy, zejména zajištění informací o kontaktních osobách ohledně přístupu k podkladům potřebným pro poskytnutí služby;
 - c. zabezpečení provozu a kapacit technických prostředků (hardware, síťová infrastruktura, operační systémy, databáze), a to minimálně těch, které jsou uvedeny ve Specifikaci díla jako předpokládané (Předpokládané kapacity Technologického centra KV);
 - d. zajištění součinnosti svých pověřených pracovníků tak, aby umožnili Zhotoviteli řádné a včasné plnění Smlouvy, přičemž požadavky na takovou součinnost musí být ze strany Zhotovitele oznámeny Objednateli s dostatečným časovým předstihem, nejdéle však 2 měsíce před dokončením díla;
 - e. umožnění Zhotoviteli (s ohledem na ochranu osobních údajů a důvěrných informací) zabezpečený vzdálený přístup do své datové sítě za účelem plnění Smlouvy, a to nejpozději do 5 pracovních dnů od účinnosti Smlouvy.

VIII. CENA DÍLA

33. Objednatel se zavazuje zaplatit Zhotoviteli za provedení Díla odměnu ve výši **8 744 400,00 Kč bez DPH** (dále jen „**Cena Díla**“).
34. Cena za provedení Díla zahrnuje veškeré náklady, jež mohou Zhotoviteli v souvislosti s poskytováním této kategorie služeb vzniknout, zejména cestovní výdaje, náklady na softwarové a hardwarové vybavení a licence. Za provedení Díla tak Zhotovitel kromě shora uvedené ceny nemá nárok na žádné další finanční plnění. Cena za provedení Díla dle Smlouvy zahrnuje veškeré náklady Zhotovitele spojené s poskytováním plnění dle Smlouvy a přiměřený zisk Zhotovitele.

IX. FAKTURACE A PLATEBNÍ PODMÍNKY

35. Objednatel se zavazuje hradit Zhotoviteli odměnu za provedení Díla na základě příslušných daňových dokladů (dále jen „**faktur**“ nebo jednotlivě „**faktura**“) vystavených Zhotovitelem.
36. Zhotovitel je oprávněn vystavit fakturu ve výši:
- a. 20 % z Ceny Díla po dokončení, předání a akceptaci všech výstupů Zhotovitele v rámci Etapy 1 – Projektování dle Specifikace Díla;
 - b. 80 % z Ceny Díla po dokončení, předání a akceptaci všech výstupů Zhotovitele v rámci Etapy 3 – Testování dle Specifikace Díla.
37. Faktura musí splňovat náležitosti daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**ZoDPH**“), včetně případné informace, že provedení Díla podléhá režimu přenesení daňové povinnosti v souladu s § 92a ZoDPH. V případě, že Zhotovitel není plátcem DPH, musí Faktura splňovat náležitosti účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. Faktura musí vždy splňovat náležitosti stanovené § 435 Občanského zákoníku.
38. Splatnost Faktury musí být stanovena tak, aby nebyla kratší než 30 dnů ode dne doručení Faktury Objednateli.
39. Stanoví-li Faktura splatnost delší, než je jako minimální stanovena v tomto článku, je Objednatel oprávněn uhradit cenu za provedení Díla nebo její část a případnou DPH ve lhůtě splatnosti určené ve Faktuře.
40. Cena za provedení Díla nebo její část a případná DPH je uhrazena vždy dnem jejich odepsání z bankovního účtu Objednatele.
41. Vyplývá-li z informací zveřejněných správcem daně ve smyslu ZoDPH, že Zhotovitel je nespolehlivým plátcem DPH, je Objednatel oprávněn příslušnou DPH uhradit přímo místně a věcně příslušnému správci daně Zhotovitele. Tento odstavec se užije pouze v případě, že Dílo nepodléhá režimu přenesení daňové povinnosti v souladu s § 92a ZoDPH.
42. Bude-li Faktura obsahovat číslo bankovního účtu určeného k úhradě ceny za provedení Díla nebo její části a případné DPH, které není správcem daně ve smyslu ZoDPH zveřejněno jako číslo bankovního účtu, které je Zhotovitelem používáno pro ekonomickou činnost, je Objednatel oprávněn uhradit cenu za provedení Díla nebo její část, na něž byla vystavena Faktura, a případnou DPH na bankovní účet zveřejněný správcem daně ve smyslu ZoDPH jako bankovní účet, který je Zhotovitelem používán pro ekonomickou činnost. Ve vztahu k Objednatelem případně hrazené DPH se tento odstavec užije pouze v případě, že Dílo nepodléhá režimu přenesení daňové povinnosti v souladu s § 92a ZoDPH.

43. Nebude-li příslušná Faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně stanovena cena za provedení Díla nebo její část, DPH nebo jiná náležitost Faktury, je Objednatel oprávněn tuto Fakturu vrátit Zhotoviteli k provedení opravy s vyznačením důvodu vrácení. Zhotovitel je povinen opravit Fakturu podle pokynů Objednatele a opravenou Fakturu neprodleně doručit Objednateli. Splatnost opravené faktury činí 30 dnů ode dne doručení Faktury Objednateli.
44. Objednatel neposkytuje Zhotoviteli žádné zálohy.

X. UKONČENÍ SMLOUVY

45. Objednatel je oprávněn, kromě případů stanovených právními předpisy, od této Smlouvy písemně odstoupit:
- a. jestliže Zhotovitel bezdůvodně nebo z důvodů na své straně přeruší provádění Díla;
 - b. jestliže Zhotovitel neodstraní v průběhu provádění Díla vady zjištěné Objednatelem, a to ani v dodatečně lhůtě stanovené písemně Objednatelem;
 - c. jestliže Zhotovitel poruší některou svoji povinnost uvedenou v odstavci 116, 117, 125, 69 až 74 nebo 75 až 80 Smlouvy;
 - d. ukáže-li se jako nepravdivé jakékoliv prohlášení Zhotovitele uvedené v odstavci 126 Smlouvy nebo ocitne-li se Zhotovitel ve stavu úpadku nebo hrozícího úpadku;
 - e. jestliže dojde k významné změně ovládání Zhotovitele podle ZOK;
 - f. jestliže dojde ke změně vlastnictví zásadních aktiv Zhotovitele, které souvisejí s plněním Smlouvy;
 - g. jestliže dojde ke změně oprávnění Zhotovitele s těmito aktivy nakládat.
46. Objednatel je oprávněn odstoupit od Smlouvy ohledně celého plnění i v případě, že Zhotovitel již zčásti plnil.
47. Smluvní strany se dále dohodly, že v případě odstoupení od Smlouvy budou zejména ujednání o odpovědnosti za škodu a nemajetkovou újmu, o sankcích, o licencích a odstavce 48 trvat i po zániku závazků ze Smlouvy.
48. Pokud před dokončením Díla dojde k odstoupení od Smlouvy, předá Zhotovitel nedokončené Dílo Objednateli písemným protokolem podepsaným oběma Smluvními stranami, ve kterém bude popsán stupeň rozpracovanosti Díla a současně předá Objednateli veškeré dokumenty získané za dobu trvání závazků ze Smlouvy, jakož i případné listiny předané Objednatelem Zhotoviteli k provedení Díla. Po vyhotovení a podepsání tohoto protokolu bude provedeno finanční vyrovnání Smluvních stran.

XI. PROVÁDĚNÍ DÍLA

49. Zhotovitel postupuje při provádění Díla samostatně a je při určení způsobu provedení Díla vázán pokyny Objednatele.
50. Změna Díla, odměny nebo dalších podmínek Smlouvy podléhá souhlasu obou Smluvních stran a bude provedena ve formě písemného dodatku ke Smlouvě.
51. Jestliže bude nutné po uzavření Smlouvy provést změny ve specifikaci Díla na základě změn obecně platných právních předpisů nebo rozhodnutí příslušných orgánů veřejné správy, aplikuje se v takovém případě ustanovení odstavce 53 Smlouvy přiměřeně.

52. Zhotovitel je povinen zajistit, aby Dílo plnilo legislativní a technické požadavky nezbytné pro plnění účelu Smlouvy.
53. V případě, že Objednatel požaduje změnu Smlouvy nebo Díla, musí Zhotovitel vypracovat a předat Objednateli podrobné hodnocení vlivů příslušné změny na odměnu, termíny provádění Díla a na další podmínky Smlouvy. Objednatel se k tomuto podrobnému zhodnocení vyjádří bez zbytečného odkladu po jeho obdržení. Schválené podrobné zhodnocení není samo o sobě dodatkem k Smlouvě, ale slouží pouze jako podklad pro jeho vypracování a uzavření.

XII. PŘEDÁNÍ A PŘEVZETÍ DÍLA

54. Předání a převzetí Díla nebo jeho dílčích částí je upraveno v podmínkách akceptace (Příloha č. 2 Smlouvy) a v tomto článku Smlouvy. Detailní návrh procesu předání a akceptace Díla včetně návrhu předávacích a akceptačních protokolů zpracuje Zhotovitel v rámci cílového konceptu řešení ve smyslu Specifikace díla a tento návrh bude v souladu s podmínkami akceptace (Příloha č. 2 Smlouvy) a tímto článkem Smlouvy.
55. O předání Díla nebo jeho dílčích částí bude mezi Smluvními stranami sepsán předávací protokol. Předávací protokol bude podepsán zástupci obou Smluvních stran. Součástí předání Díla nebo jeho dílčích částí, není-li ve Smlouvě stanoveno jinak, je zejména:
- a. kontrola funkčnosti implementace Díla nebo jeho dílčí části s možností ovládání jeho uživateli;
 - b. zaškolení odborných osob Objednatele (v potřebném rozsahu);
 - c. předání požadované dokumentace Díla nebo jeho dílčí části.
56. Podepsáním předávacího protokolu je zahájen proces akceptace Díla nebo jeho dílčí části. Objednatel je povinen do 30 dnů od zahájení procesu akceptace zajistit provedení testů nebo upozornit Zhotovitele na případné zjištěné vady Díla nebo jeho dílčí části. U Díla jako celku proběhne testování v rámci Etapy 3 – Testování, u dílčích částí Díla předávaných před jeho úplným dokončením proběhne testování v rámci Etapy 2 – Vývoj a implementace, je-li pro dílčí část Díla stanoveno testování. Pokud Objednatel nezajistí provedení testů nebo nestihne upozornit Zhotovitele na zjištěné vady Díla nebo jeho dílčí části ve lhůtě dle druhé věty tohoto odstavce, nepovažuje se Dílo nebo jeho dílčí část bez dalšího za akceptované. Podmínky akceptace jsou blíže upraveny v příloze Smlouvy (Příloha č. 2 Smlouvy). Úspěšný proces akceptace Díla nebo jeho dílčí části je ukončen podpisem akceptačního protokolu.
57. Pokud Objednatel Dílo nebo jeho dílčí část neakceptuje, je povinen vystavit protokol o odmítnutí akceptace se specifikací důvodů odmítnutí. Pokud bude příčina na straně Zhotovitele, zajistí Zhotovitel, aby Dílo nebo jeho dílčí část odpovídalo požadavkům uvedeným ve Smlouvě, a to ve lhůtě uvedené v protokolu o odmítnutí akceptace, která bude činit minimálně 15 dnů. Po provedení úprav Díla se bude opakovat postup uvedený v odstavci 55 a 56 této Smlouvy, a to až do okamžiku akceptace Díla nebo jeho dílčí části.

XIII. SMLUVNÍ SANKCE

58. Zhotovitel bere na vědomí, že Dílo je nezbytné pro řádný provoz systému elektronického odbavení cestujících v integrovaném dopravním systému Veřejné dopravy Vysočiny. Z tohoto důvodu je kladen zvýšený důraz na dodržení doby a kvality plnění.

59. Jestliže se dostane Zhotovitel do prodlení s provedením Díla v termínu uvedeném v odstavci 9 Smlouvy, je povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z ceny za provedení Díla podle odstavce 33 Smlouvy za každý započatý den prodlení. Jestliže doba prodlení přesáhne 60 dnů, je Objednatel oprávněn od této Smlouvy odstoupit.
60. Poruší-li Zhotovitel dílčí termíny plnění pro předání dílčích částí Díla podle podrobného harmonogramu plnění ve smyslu odstavce 10 Smlouvy, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,05 % z ceny za provedení Díla podle odstavce 33 Smlouvy za každý započatý den prodlení.
61. Poruší-li Zhotovitel povinnost odstranit ve sjednané lhůtě vady Díla podle odstavce 57 Smlouvy, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,05 % z ceny za provedení Díla podle odstavce 33 Smlouvy za každý započatý den prodlení až do okamžiku předání Díla, o kterém bude Zhotovitel mít za to, že vady Díla byly odstraněny. Pokud se však v průběhu opakované akceptace ukáže, že vady Díla nebyly ve smyslu odstavce 57 Smlouvy řádně odstraněny, je Zhotovitel povinen zaplatit Objednateli jednorázovou smluvní pokutu ve výši 50.000,- Kč.
62. Jestliže Zhotovitel poruší kteroukoliv z povinností uvedených v článku V Smlouvy nebo podle odstavce 116, 117, 125, 69 až 74 a 75 až 80 Smlouvy, je povinen zaplatit Objednateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení.
63. Poruší-li Objednatel povinnost uhradit Fakturu nebo zaplatit cenu za provedení Díla ve sjednané době, je povinen uhradit Zhotoviteli zákonný úrok z prodlení ve výši podle právních předpisů.
64. Zaplacení smluvní pokuty nezbavuje Zhotovitele povinnosti splnit dluh smluvní pokutou utvrzený.
65. Objednatel je oprávněn požadovat náhradu škody a nemajetkové újmy způsobené porušením povinností Zhotovitele, na kterou se vztahuje smluvní pokuta, v plné výši.
66. Splatnost smluvních pokut podle Smlouvy bude 15 dnů od doručení písemné výzvy k zaplacení smluvní pokuty straně povinné.
67. Pro vyloučení pochybností se stanoví, že je umožněn souběh více smluvních pokut vedle sebe.

XIV. ODPOVĚDNOST ZHOTOVITELE

68. Zhotovitel odpovídá za veškeré škody a nemajetkové újmy, které vzniknou Objednateli v důsledku porušení Smlouvy Zhotovitelem. Zhotovitel je povinen nahradit takto vzniklou škodu a nemajetkovou újmu v plném rozsahu, včetně případných sankcí udělených Objednateli orgány veřejné moci, jejichž příčinou bylo porušení povinností Zhotovitele dle Smlouvy.

XV. PODDODAVATELÉ

69. Zhotovitel je oprávněn pověřit plněním svých povinností vyplývajících ze Smlouvy pouze jiné osoby uvedené v seznamu poddodavatelů (Příloha č. 3 Smlouvy), nebo osoby písemně odsouhlasené Objednatel (dále jen jednotlivě „**Poddodavatel**“ nebo společně „**Poddodavatelé**“).
70. Zhotovitel odpovídá za plnění Poddodavatele tak, jako by plnil sám.
71. Zhotovitel prohlašuje a zavazuje se, že jako ručitel uspokojí za jakéhokoliv Poddodavatele jeho povinnost nahradit újmu způsobenou Poddodavatelem Objednateli při plnění nebo v souvislosti s

plněním povinností ze Smlouvy, jestliže Poddodavatel povinnost k náhradě újmy nesplní. Objednatel Zhotovitele jako ručitele podle předchozí věty přijímá.

72. Zhotovitel se zavazuje, že Poddodavatelé, kterými prokazoval splnění kvalifikace v Řízení Veřejné zakázky, se budou podílet na plnění povinností Zhotovitele vyplývajících ze Smlouvy v rozsahu podle nabídky Zhotovitele podané do Řízení Veřejné zakázky.
73. Objednatel je oprávněn požadovat a Zhotovitel je povinen zabezpečit změnu Poddodavatele, a to v případech, kdy:
- a. bude Poddodavatel vůči Objednateli v prodlení se splněním povinnosti z jiného závazku nebo
 - b. bude Poddodavatel pravomocně odsouzen za trestný čin nebo
 - c. se Poddodavatel ocitne ve stavu úpadku nebo hrozícího úpadku nebo
 - d. bude Poddodavateli uložen zákaz plnění veřejných zakázek nebo
 - e. bude dán jiný závažný důvod pro změnu Poddodavatele.

Zhotovitel je povinen navrhnout nového Poddodavatele do 10 dnů od doručení žádosti Objednatele. Pokud Zhotovitel v Řízení Veřejné zakázky prokazoval původním Poddodavatelem kvalifikaci, nový Poddodavatel musí splňovat kvalifikaci stanovenou v Řízení Veřejné zakázky prokazovanou původním nahrazovaným Poddodavatelem a musí doložit příslušné doklady prokazující splnění této kvalifikace. Nový Poddodavatel musí být odsouhlasen Objednatelem postupem obdobným postupu podle odstavce 74 Smlouvy.

74. Zhotovitel je oprávněn změnit Poddodavatele z důvodů na straně Zhotovitele pouze s předchozím písemným souhlasem Objednatele. Objednatel vydá písemný souhlas se změnou do 10 dnů od doručení žádosti Zhotovitele. Objednatel souhlas se změnou nevydává, pokud:
- a. prostřednictvím původního Poddodavatele Zhotovitel v Řízení veřejné zakázky prokazoval kvalifikaci a nový Poddodavatel nebude mít stejnou či vyšší kvalifikaci jako původní nahrazovaný Poddodavatel nebo
 - b. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil.

XVI. ČLENOVÉ REALIZAČNÍHO TÝMU

75. Zhotovitel je oprávněn pověřit prováděním vyhrazených činností při provádění Díla pouze osoby uvedené v seznamu členů realizačního týmu (Příloha č. 4 Smlouvy), nebo osoby písemně odsouhlasené Objednatelem (dále jen jednotlivě „*Člen realizačního týmu*“ nebo společně „*Členové realizačního týmu*“).
76. Vyhrazenými činnostmi při provádění Díla jsou:
- a. vedení projektu realizace Díla za Zhotovitele – výkon funkce Manažer projektu,
 - b. vedení přípravy detailní prováděcí dokumentace k Dílu – výkon funkce Systémový architekt,
 - c. vedení vývoje software v rámci Díla – výkon funkce Pracovník vývoje software.
77. Členové realizačního týmu musí být po celou dobu plnění Smlouvy způsobilí k výkonu činností, kterými jsou v rámci plnění Smlouvy pověřeni, a to zejména podle příslušných právních předpisů.
78. Zhotovitel se zavazuje, že Členové realizačního týmu, kterými prokazoval splnění kvalifikace v Řízení veřejné zakázky, se budou podílet na plnění povinností Zhotovitele vyplývajících ze Smlouvy v rozsahu podle nabídky Zhotovitele podané do Řízení veřejné zakázky.

79. Objednatel je oprávněn požadovat a Zhotovitel je povinen zabezpečit změnu Člena realizačního týmu, a to v případech, kdy:
- a. bude činnost Člena realizačního týmu nedostatečná nebo neuspokojivá nebo
 - b. kontrola, obecná bezpečnost, organizace a koordinace provádění Díla nejsou dostatečné nebo uspokojivé nebo
 - c. kvalita dodávek a služeb neodpovídá požadavkům Smlouvy nebo
 - d. nejsou vykonávány pokyny Objednatele vydané podle Smlouvy nebo
 - e. bude Člen realizačního týmu vůči Objednateli v prodlení se splněním povinnosti z jiného závazku nebo
 - f. Člen realizačního týmu přestane být způsobilý k výkonu své funkce v realizačním týmu nebo
 - g. bude Člen realizačního týmu pravomocně odsouzen za trestný čin nebo
 - h. se Člen realizačního týmu ocitne ve stavu úpadku nebo hrozícího úpadku nebo
 - i. bude Členu realizačního týmu uložen zákaz plnění veřejných zakázek nebo
 - j. bude dán jiný závažný důvod pro změnu Člena realizačního týmu.
- Zhotovitel je povinen navrhnout nového Člena realizačního týmu do 10 dnů od doručení žádosti Objednatele. Pokud Zhotovitel v Řízení Veřejné zakázky prokazoval původním Členem realizačního týmu kvalifikaci, nový Člen realizačního týmu musí splňovat kvalifikaci stanovenou v Řízení Veřejné zakázky prokazovanou původním nahrazovaným Členem realizačního týmu a musí doložit příslušné doklady prokazující splnění této kvalifikace. Nový Člen realizačního týmu musí být odsouhlasen Objednatelem postupem obdobným postupu podle odstavce 80 Smlouvy.
80. Zhotovitel je oprávněn změnit Člena realizačního týmu z důvodů na straně Zhotovitele pouze s předchozím písemným souhlasem Objednatele. Objednatel vydá písemný souhlas se změnou do 10 dnů od doručení žádosti Zhotovitele. Objednatel souhlas se změnou nevydává, pokud:
- a. prostřednictvím původního Člena realizačního týmu Zhotovitel v Řízení Veřejné zakázky prokazoval kvalifikaci a nový Člen realizačního týmu nebude mít stejnou či vyšší kvalifikaci jako původní nahrazovaný Člen realizačního týmu nebo
 - b. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil (zejm., kdyby nový Člen realizačního týmu měl obdržet v rámci hodnocení nabídek v Řízení Veřejné zakázky méně bodů, než obdržel nahrazovaný Člen realizačního týmu).

XVII. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA

81. V případě, že součástí plnění Zhotovitele dle Smlouvy jsou movité věci, které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto věcem dnem podpisu příslušného protokolu o předání. Ke stejnému dni přechází na Objednatele také nebezpečí škody na předaných věcech. Do okamžiku nabytí vlastnického práva uděluje Zhotovitel Objednateli právo tyto věci užívat v rozsahu a způsobem, který vyplývá z účelu této Smlouvy.
82. Bude-li výsledkem plnění Zhotovitele dle Smlouvy předmět naplňující znaky autorského díla (dále jen „*Autorské dílo*“ či „*Autorská díla*“) ve smyslu autorského zákona, nabývá Objednatel dnem poskytnutí Autorského díla Objednateli k užívání dle této Smlouvy právo užívat takové Autorské dílo (dále jen „*Licence*“).
83. Licence se poskytuje, resp. musí být poskytnuta:
- a. jako úplatná, přičemž úplata je zahrnuta v ceně za provedení Díla dle odst. 33 Smlouvy;
 - b. jako nevýhradní;
 - c. z hlediska časového rozsahu minimálně na dobu trvání všech majetkových práv k předmětu Licence;
 - d. z hlediska územního rozsahu jako neomezená;

- e. z hlediska věcného rozsahu (způsobu užití) tak, že opravňuje ke všem známým a možným způsobům užití, které povaha Díla připouští, a které nejsou v rozporu s právními předpisy, zejména k takovým způsobům užití, jež jsou potřebná nebo nezbytná k tomu, aby bylo Dílo možné užívat k účelu sjednanému Smlouvou nebo účelu ze Smlouvy vyplývajícimu;
 - f. z hlediska osobního rozsahu (multilicence), resp. množství jako neomezená.
84. Objednatel není povinen Licenci využít.
85. Zhotovitel tímto jménem všech autorů Autorských děl:
- a. bezplatně uděluje Objednateli oprávnění Autorská díla zveřejnit a jakýmkoliv způsobem měnit, tedy zejm. je jakkoliv upravovat, dělit, rozšiřovat, spojovat s díly jinými, zařadit do díla souborného apod.;
 - b. zmocňuje Objednatele, aby jménem všech autorů Autorských děl uděloval třetím osobám oprávnění Autorská díla zveřejnit a jakýmkoliv způsobem měnit, tedy zejm. je jakkoliv upravovat, dělit, rozšiřovat, spojovat s díly jinými, zařadit do díla souborného apod.;
 - c. uděluje Objednateli oprávnění zmocnit jménem všech autorů Autorských děl třetí osoby k udělení oprávnění jiným třetím osobám ke zveřejnění nebo jakékoliv změně Autorských děl v rozsahu dle písm. a tohoto odstavce.
86. V případě zániku Smlouvy jinak než splněním, nabývá Objednatel oprávnění dle odst. 85 k doposud dodaným Autorským dílům okamžikem zániku Smlouvy.
87. Součástí Licence je rovněž neomezené právo Objednatele poskytnout třetím osobám podlicenci k užití Autorského díla v rozsahu shodném s rozsahem Licence a souhlas Zhotovitele k postoupení Licence na třetí osoby a nepožaduje sdělení, zda a komu byla Licence (podlicence) poskytnuta nebo postoupena.
88. Licence se automaticky vztahuje i na všechny nové verze, aktualizované verze, i na úpravy a překlady Autorského díla poskytnuté Zhotovitelem.
89. Poskytuje-li Zhotovitel Licenci k počítačovým programům vyvíjeným Zhotovitelem (popř. jeho poddodavatelem či jinou třetí osobou), vztahuje se Licence ve stejném rozsahu k počítačovým programům ve zdrojovém a strojovém kódu, jakož i ke koncepčním přípravným materiálům, a to i na případné další verze počítačových programů. Zdrojové kódy budou Objednateli poskytnuty za podmínek stanovených v čl. XVIII Smlouvy.
90. Do té doby, než bude Autorské dílo poskytnuto Objednateli k užívání dle odst. 82 Smlouvy je Objednatel oprávněn Autorské dílo užívat v rozsahu a způsobem nezbytným k provedení akceptace výsledku plnění Zhotovitele dle Smlouvy.
91. Smluvní strany výslovně prohlašují, že pokud při poskytování plnění dle Smlouvy vznikne činností Zhotovitele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Zhotovitel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena za provedení Díla je stanovena se zohledněním tohoto ustanovení a Zhotoviteli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.
92. Bude-li Autorské dílo vytvořeno činností Zhotovitele, Smluvní strany činí nesporným, že jakékoliv takové Autorské dílo vzniklo z podnětu a pod vedením Objednatele.

93. Součástí výsledku plnění Zhotovitele dle Smlouvy může být tzv. proprietární (standardní) software (dále jen „**Proprietární software**“), u kterého Zhotovitel nemůže Objednateli poskytnout oprávnění dle předchozích ustanovení tohoto článku Smlouvy nebo to po něm nelze spravedlivě požadovat, to však pouze při splnění některé z následujících podmínek:
- a. jedná se o software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi na sobě nezávislými a vzájemně nepropojenými subjekty oprávněnými takovýto software upravovat, a který je v době uzavření smlouvy prokazatelně užíván v produktivním prostředí nejméně u deseti na sobě nezávislých a vzájemně nepropojených subjektů. Zhotovitel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat;
 - b. jedná se o tzv. open source software, který je veřejnosti poskytován zdarma, včetně detailně komentovaných zdrojových kódů, úplné uživatelské, provozní a administrátorské dokumentace a práva software měnit. Zhotovitel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat;
 - c. jedná se o software, u kterého Zhotovitel poskytne s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v rámci výsledku plnění Zhotovitele dle této Smlouvy bez nutnosti vynakládání výraznějších prostředků, písemnou garanci, že další rozvoj výsledku plnění Zhotovitele dle této Smlouvy jinou osobou než Zhotovitelem je možné provádět bez toho, aby tím byla dotčena práva autorů takového softwaru, neboť nebude nutné zasahovat do zdrojových kódů takového softwaru anebo proto, že případné nahrazení takového softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele;
 - d. jedná se o software, k němuž Zhotovitel Objednateli poskytne nebo zprostředkuje poskytnutí úplných komentovaných zdrojových kódů a bezpodmínečného práva provádět jakékoliv modifikace, úpravy, změny takového software a dle svého uvážení do něj zasahovat, zpracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob, přičemž poskytování zdrojových kódů se řídí čl. XVIII Smlouvy.
94. V případě Proprietárního softwaru je dostatečné, aby Zhotovitel Objednateli poskytl neomezené nevýhradní právo užívat takový Proprietární software jakýmkoli způsobem nejméně po dobu 10 let od akceptace Díla, a v množstevním rozsahu, který je nezbytný pro pokrytí potřeb Objednatele ke dni předání předmětného výsledku plnění Zhotovitele dle Smlouvy Objednateli, a to včetně práva Objednatele do Proprietárního softwaru zasahovat, pokud tak stanoví příslušné ustanovení odst. 93 Smlouvy. V případě výpovědi či odstoupení od Smlouvy se Zhotovitel zavazuje nabídnout Objednateli právo užívat Proprietární software v rozsahu, v jakém je to nezbytné pro řádné užívání výsledků plnění Zhotovitele dle Smlouvy. Tím není dotčeno právo Objednatele pořídit Proprietární software i od třetí osoby bez ohledu na licence pořízené dříve Zhotovitelem. V případě využití tohoto přednostního práva se Zhotovitel zavazuje, že právo užívat Proprietární software dle tohoto odstavce této Smlouvy nabídne Objednateli za běžných tržních podmínek a bude vycházet z účetní hodnoty licencí, které pořídil.
95. Nelze-li to na Zhotoviteli spravedlivě požadovat, nemusí být Objednateli k Proprietárnímu softwaru předány zdrojové kódy a stejně tak nemusí být poskytnuto právo Objednatele do Proprietárního softwaru zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská a provozní dokumentace.
96. Zhotovitel se zavazuje samostatně zdokumentovat veškeré využití Proprietárního software v rámci jím poskytnutých výsledků plnění dle této Smlouvy a předložit Objednateli ucelený přehled využitého Proprietárního software, jeho licenčních podmínek a jeho alternativních dodavatelů. Tento přehled je Zhotovitel povinen předložit Objednateli vždy do 3 (tří) pracovních dnů po

akceptaci výsledku plnění, v jehož rámci Zhotovitel využil Proprietární software a dále vždy do 1 (jednoho) měsíce od doručení výzvy Objednatele, kterou může Objednatel učinit kdykoli, nejpozději však do 3 (tří) kalendářních let po roku, ve kterém skončilo trvání této Smlouvy.

97. Jestliže jsou s užitím Proprietárního software či jiných souvisejících plnění spojeny jednorázové či pravidelné poplatky, je Zhotovitel povinen v rámci ceny za provedení Díla řádně uhradit všechny tyto poplatky za celou dobu trvání licence.
98. Udělení Licence nelze ze strany Zhotovitele vypovědět a její účinnost trvá i po skončení účinnosti Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak.
99. Odměna za zprostředkování nebo postoupení Licence k Autorskému dílu je zahrnuta v ceně za služby, při jejichž poskytnutí došlo k vytvoření Autorského díla.
100. Práva získaná v rámci plnění Smlouvy přecházejí i na případného právního nástupce Objednatele. Případná změna v osobě Zhotovitele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci Smlouvy Zhotovitelem Objednateli.
101. Zhotovitel je povinen postupovat tak, aby udělení Licence k Autorskému dílu dle Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.
102. Zhotovitel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k Autorským dílům, která jsou výsledkem plnění Zhotovitele dle Smlouvy, resp. že má souhlas všech relevantních třetích osob k poskytnutí Licence k Autorským dílům podle tohoto článku Smlouvy; toto prohlášení zahrnuje i taková práva, která by vytvořením Autorského díla teprve vznikla.
103. Zhotovitel prohlašuje, že je oprávněn zmocnění a oprávnění dle odst. 85 Smlouvy a Licenci ve shora uvedeném rozsahu Objednateli poskytnout a udělit. Objednatel oprávnění a zmocnění dle odst. 85 Smlouvy přijímá. Zhotovitel jménem všech autorů Autorských děl s Objednatelem sjednává, že autoři Autorských děl jsou oprávněni odvolat zmocnění dle odst. 85 Smlouvy jen v případě, že by Objednatel při výkonu zástupčího oprávnění postupoval v rozporu s dobrými mravy.
104. Zhotovitel prohlašuje, že veškeré jím poskytnuté plnění dle Smlouvy je prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění. V případě, že by nárok třetí osoby vznikl v souvislosti s poskytnutým plněním Zhotovitele dle Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání poskytnutého plnění dle Smlouvy, zavazuje se Zhotovitel zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu plnění sjednanou dle Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.
105. Zhotovitelem udělená Licence se vztahuje ve shora uvedeném rozsahu i na jakákoli rozšíření, upgrady, updaty a patche Autorských děl.
106. Zhotovitel je ve vztahu k software dále povinen:
 - a. v rámci Etapy 1 – Projektování dle Specifikace Díla předat Objednateli seznam veškerého na Díle použitého software;
 - b. v rámci Etapy 2 – Vývoj a implementace dle Specifikace Díla předat Objednateli dokumentaci k veškerému na Díle použitému software.

XVIII. ZDROJOVÝ KÓD

107. Zhotovitel je povinen současně s předáním Díla, resp. těch částí Díla, které jsou počítačovým programem, předat Objednateli zdrojový kód Díla (dále jen „**Zdrojový kód**“). Zdrojový kód dle Smlouvy bude strukturovaný, dokumentovaný a komentovaný, přičemž bude možné jej přeložit a sestavit do spustitelných programů. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručovat možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace Zdrojového kódu takovéto části plnění dle Smlouvy. Zdrojový kód bude Objednateli Zhotovitelem předán do vhodného elektronického uložení zřízeného Zhotovitelem pro tento účel. O předání Zdrojového kódu bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.
108. Povinnost Zhotovitele uvedená v odstavci 107 Smlouvy se přiměřeně použije i pro jakékoliv modifikace, úpravy, opravy, změny, doplnění, upgrade nebo update Zdrojového kódu počítačového programu tvořícího Dílo, k nimž dojde při plnění Smlouvy nebo v rámci odstraňování vad Díla. Dokumentace změny Zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do Zdrojového kódu. Pro evidenci změn Zdrojového kódu je možné využít specializovaných nástrojů pro verzování změn. Zhotovitel bude odpovídat za aktuální stav obsahu Zdrojového kódu.
109. Zhotovitel je povinen předat Objednateli dokumentovanou změnu Zdrojového kódu nejpozději do 7 kalendářních dnů následujících po dni, ve kterém byla změna Zdrojového kódu uskutečněna. V případě jakéhokoli ukončení Smlouvy z důvodu porušení Smlouvy Zhotovitelem je Zhotovitel povinen předat Objednateli aktuální Zdrojové kódy a koncepční přípravné materiály všech součástí Díla tak, aby byl Objednatel držitelem Zdrojového kódu minimálně k v dané chvíli aktuální verzi Díla.
110. Zhotovitel bere na vědomí, že Objednatel může Zdrojový kód dle odstavce 107 Smlouvy či jeho změny sdílet s třetí osobou, je-li to nezbytné pro zajištění řádného fungování EOC.
111. Zhotovitel bere na vědomí, že Objednatel může Zdrojový kód dle odstavce 107 Smlouvy užít či zpřístupnit pro provádění modifikací, úprav, změn a rozvoje autorského díla dle článku XVII. Smlouvy třetím osobám.

XIX. PRÁVA K DATABÁZÍM

112. Ve vztahu k databázím Objednatele platí:
- Smluvní strany prohlašují, že práva k veškerým databázím Objednatele existujícím před uzavřením této Smlouvy nebo vytvořeným Objednatelům kdykoliv v průběhu plnění Smlouvy, které mají být využity Zhotovitelem pro účely plnění Smlouvy, náleží Objednateli, který je pořizovatelem databáze ve smyslu § 89 Autorského zákona;
 - Objednatel v souvislosti s plněním dle této Smlouvy nepřevádí práva pořizovatele databáze ve smyslu § 90 odst. 6 Autorského zákona.
113. Ve vztahu k databázím vytvořeným pro potřeby Smlouvy platí:
- Smluvní strany prohlašují, že práva k veškerým databázím vytvořeným Zhotovitelem pro účely plnění této Smlouvy náleží Objednateli, který je pořizovatelem databáze ve smyslu § 89 Autorského zákona;
 - Objednatel v souvislosti s plněním dle Smlouvy nepřevádí práva pořizovatele databáze ve smyslu § 90 odst. 6 Autorského zákona.

114. Smluvní strany potvrzují, že s ohledem na práva Objednatele k databázím specifikovaným v odstavcích 112 a 113 této Smlouvy je Zhotovitel oprávněn užívat databáze pouze v rozsahu a způsobem nezbytným pro provoz, správu a rozvoj předmětu plnění dle Servisní smlouvy.
115. Součástí práva k databázím dle odstavců 112 a 113 Smlouvy je též právo Objednatele vytěžovat a zužitkovávat celý obsah databází za účelem jeho zpracování pro výsledné zobrazení výsledku zpracování.

XX. POJIŠTĚNÍ

116. Zhotovitel se zavazuje, že bude mít po celou dobu trvání závazku vyplývajícího ze Smlouvy až do okamžiku akceptace Díla sjednáno pojištění odpovědnosti za škodu či jinou újmu způsobenou Zhotovitelem při výkonu činnosti jiné osobě s limitem pojistného plnění minimálně ve výši 20.000.000,- Kč. V případě, že Smlouvu uzavřelo na straně Zhotovitele více osob (členů sdružení, členů společnosti apod.), musí pojistná smlouva prokazatelně pokrývat případnou škodu či jinou újmu způsobenou kteroukoli z těchto osob.
117. Zhotovitel je povinen předložit Objednateli pojistnou smlouvu nebo pojistku osvědčující splnění povinnosti Zhotovitele podle předchozího odstavce Smlouvy kdykoli v průběhu trvání závazků ze Smlouvy bezodkladně poté, kdy k tomu bude Objednatelem vyzván.
118. Zhotovitel i Objednatel se zavazují uplatnit pojistnou událost u pojišťovny bez zbytečného odkladu.

XXI. ZÁVĚREČNÁ USTANOVENÍ

119. Tvoří-li Zhotovitele více osob, platí následující:
- všechny osoby tvořící Zhotovitele jsou ze Smlouvy zavázány společně a nerozdílně,
 - jednání kterékoli z osob tvořících Zhotovitele je přičítáno Zhotoviteli bez ohledu na vnitřní vztahy mezi jednotlivými osobami tvořícími Zhotovitele,
 - za Zhotovitele může jednat kterákoli z osob tvořících Zhotovitele.
120. Zhotovitel je povinen neprodleně písemně informovat Objednatele o skutečnostech majících i potenciálně vliv na plnění jeho povinností vyplývajících ze Smlouvy, a není-li to možné, nejpozději následující den poté, kdy příslušná skutečnost nastane nebo Zhotovitel zjistí, že by nastat mohla. Současně je Zhotovitel povinen učinit veškeré nezbytné kroky vedoucí k eliminaci případné škody hrozící Objednateli, a to zejména obstarat neprodleně náhradní plnění, přičemž je povinen nést případný rozdíl ceny.
121. Zhotovitel je povinen chránit Dílo a majetek Objednatele a bude odpovědný za škody, které vzniknou z jeho činnosti v souvislosti s prováděním Díla. Způsobí-li Zhotovitel při provádění Díla škodu na Díle, jiném majetku Objednatele nebo majetku jiné osoby, bude odpovědný za uvedení v předešlý stav na vlastní náklady, a není-li to dobře možné nebo žádá-li to poškozený, pak za náhradu takové škody.
122. Zhotovitel bere na vědomí, že Objednatel je povinným subjektem podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
123. Zhotovitel je povinen archivovat veškerou dokumentaci související s plněním ze Smlouvy včetně účetních dokladů, a to po dobu 10 let od zániku závazků vyplývajících ze Smlouvy, a kdykoli po tuto dobu umožnit Objednateli přístup k této dokumentaci.

124. Zhotovitel je povinen minimálně po dobu stanovenou v předchozím odstavci poskytovat požadované informace a dokumentaci související s plněním Smlouvy zaměstnancům nebo zmocněncům pověřených orgánů (Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci Díla a poskytnout jim při provádění kontroly součinnost.
125. Zhotovitel je při plnění Smlouvy povinen zajistit důstojné pracovní podmínky, bezpečnost práce, dodržování veškerých právních předpisů, zejména pak zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy) a zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění Smlouvy budou podílet.
126. Zhotovitel prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Zhotovitel dále prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek Zhotovitele a že mu není známo, že by vůči němu takové řízení bylo zahájeno.
127. Vzhledem k veřejnoprávnímu charakteru Objednatele Zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním Smlouvy v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.
128. Smluvní strany prohlašují, že identifikační údaje uvedené v článku I Smlouvy odpovídají aktuálnímu stavu a že osobami jednajícími při uzavření Smlouvy jsou osoby oprávněné k jednání za Smluvní strany bez jakéhokoliv omezení vnitřními předpisy Smluvních stran.
129. Jakékoliv změny údajů uvedených v článku I Smlouvy, jež nastanou v době po uzavření Smlouvy, jsou Smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé Smluvní straně.
130. V případě, že se kterékoliv prohlášení některé ze Smluvních stran uvedené ve Smlouvě ukáže býti nepravdivým, odpovídá tato Smluvní strana za škodu a nemajetkovou újmu, které nepravdivostí prohlášení nebo v souvislosti s ní druhé Smluvní straně vznikly.
131. Zhotovitel souhlasí se zveřejněním Smlouvy v souladu s povinnostmi Objednatele za podmínek vyplývajících z příslušných právních předpisů, zejména souhlasí se zveřejněním Smlouvy, včetně všech jejích změn a dodatků, výše skutečně uhrazené ceny na základě Smlouvy a dalších údajů na profilu zadavatele Objednatele podle § 219 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**Zákon o registru smluv**“). Zhotovitel prohlašuje, že Smlouva ani žádná její část nejsou obchodním tajemstvím Zhotovitele ve smyslu § 504 Občanského zákoníku. Smlouvu podle vůle Smluvních stran na profilu zadavatele a v registru smluv v souladu s příslušnými právními předpisy, zejména ve lhůtách stanovených příslušnými právními předpisy, uveřejní Objednatel.
132. Zhotovitel je povinen chránit osobní údaje a při jejich ochraně postupovat v souladu s příslušnými právními předpisy, zejména zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů a Nařízením evropského parlamentu a rady (EU) 2016/679 ze dne 27.04.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

133. Zhotovitel není oprávněn postoupit žádnou svou pohledávku za Objednatelům vyplývající ze Smlouvy nebo vzniklou v souvislosti se Smlouvou.
134. Zhotovitel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelům vyplývající ze Smlouvy nebo vzniklé v souvislosti se Smlouvou na jakoukoliv pohledávku Objednatel za Zhotovitelem.
135. Objednatel je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Zhotovitelem vyplývající ze Smlouvy nebo vzniklé v souvislosti se Smlouvou (zejména smluvní pokutu) na jakoukoliv splatnou i nesplatnou pohledávku Zhotovitele za Objednatel.
136. Poruší-li Zhotovitel v souvislosti se Smlouvou jakoukoli svoji povinnost, nahradí Objednateli škodu a nemajetkovou újmu z toho vzniklou. Povinnosti k náhradě se Zhotovitel zproští, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Zhotovitele nebo vzniklá až v době, kdy byl Zhotovitel s plněním povinnosti v prodlení, ani překážka, kterou byl Zhotovitel povinen překonat, jej však povinnosti k náhradě nezproští.
137. Veškerá práva a povinnosti Smluvních stran vyplývající ze Smlouvy se řídí českým právním řádem. Smluvní strany se dohodly, že ustanovení právních předpisů, která nemají donucující účinky, mají přednost před obchodními zvyklostmi, pokud Smlouva nestanoví jinak.
138. Tato Smlouva představuje úplnou dohodu Smluvních stran ohledně předmětu Smlouvy.
139. Tato Smlouva může být měněna nebo doplňována pouze na základě písemných dodatků podepsaných oběma Smluvními stranami.
140. Veškeré přílohy této Smlouvy jsou její neoddělitelnou součástí.
141. Veškeré spory vznikající ze Smlouvy nebo v souvislosti s ní, které se nepodaří vyřešit dohodou Smluvních stran, budou rozhodovány věcně a místně příslušnými obecnými soudy České republiky.
142. Písemnou formou se rozumí listina podepsaná oprávněnou osobou Smluvní strany, e-mail podepsaný uznávaným elektronickým podpisem oprávněné osoby Smluvní strany, nebo datová zpráva zaslaná prostřednictvím datové schránky Smluvní strany.
143. Veškerá písemná komunikace mezi Objednatel a Zhotovitelem musí probíhat v elektronické podobě a veškeré dokumenty (vč. faktur) je Zhotovitel povinen Objednateli předávat v elektronické podobě, nebude-li to vzhledem k povaze komunikace nebo předávaných dokumentů vytvářet Smluvním stranám nepřiměřené obtíže.
144. Smlouva je uzavírána v elektronické podobě a je podepisována uznávaným elektronickým podpisem ve smyslu zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.
145. Smlouva nabývá platnosti dnem jejího uzavření a účinnosti dnem jejího zveřejnění v registru smluv.

146. Nedílnou součástí této Smlouvy je

- | | |
|---------------------|---|
| Příloha č. 1 | Specifikace díla |
| Příloha č. 2 | Podmínky akceptace |
| Příloha č. 3 | Seznam poddodavatelů |
| Příloha č. 4 | Seznam členů realizačního týmu |
| Příloha č. 5 | Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele |

DOLOŽKA

podle § 23 zákona č. 129/2000 Sb., o krajích, v platném znění

Tato Smlouva byla schválena Radou Kraje Vysočina na jednání konaném dne 09.01.2024, usnesením č. 0013/01/2024/RK nadpoloviční většinou hlasů všech členů rady kraje.

V Jihlavě dne dle el. podpisu

V Praze dne dle el. podpisu

Objednatel

Zhotovitel

**Ing. Miroslav
Houška**

Digitálně podepsal Ing.
Miroslav Houška
Datum: 2024.01.22 07:24:23
+01'00'

Příloha č. 1
Smlouvy o dílo

Specifikace díla



**Technická zadávací dokumentace na systém odbavení cestujících
v integrovaném dopravním systému Veřejná doprava Vysočiny**

Elektronické odbavení cestujících VDV

**Využití důvěryhodného identifikátoru ve formě nosiče dopravního
produktu**

Požadavky na řešení

Verze 2.1

Obsah

Obsah.....	2
1 Použité zkratky a pojmy.....	4
2 Úvod.....	5
3 Obecné požadavky.....	6
4 Typy identifikátorů v systému EOC.....	12
4.1 Bezkontaktní bankovní karta	12
4.2 QR kód generovaný mobilní aplikací	13
4.3 Bezkontaktní čipové karty vydávané dopravcem	14
5 Požadavky na samoobslužný systém pro odbavení zákazníků (portál zákazníka, e-shop).....	17
5.1 Základní funkce	17
5.2 Životní cyklus uživatele systému.....	18
5.3 Správa uživatelského profilu cestujícího	19
5.4 Registrace identifikátorů	19
5.5 Výběr a úhrada produktu	19
5.5.1 Výběr dle tarifu	20
5.5.2 Výběr pomocí kalkulatoru jízdného.....	20
5.5.3 Výběr pomocí vyhledávače spojení	20
5.6 Správa zakoupených produktů	20
6 Požadavky na systém administrace	22
6.1 Základní funkce	22
6.2 Správa subjektů a dopravců	22
6.3 Správa číselníků	22
6.4 Správa tarifu	24
6.5 Správa subjektů a dopravců jako uživatelů systému.....	24
6.6 Správa prodejních míst	25
6.7 Správa sestav	26
7 Požadavky na prodejní portál (prodejní místo –předprodej u dopravce)	28
7.1 Požadované funkcionality prodejního portálu	28
7.2 Ověřování uživatele (cestujícího)	28
7.3 Správa identifikátorů uživatele (cestujícího)	28
7.4 Správa zákaznických (uživatelských) profilů cestujících	29
7.5 Prodej dopravních produktů.....	29
7.6 Prodej doplňkových produktů	30
7.7 Účetní a statistické sestavy.....	30
8 Požadavky na systém mobilních zařízení pro revizory	31

9	Popis whitelistů.....	35
9.1	Základní definice struktury dat	35
9.2	Zabezpečení osobních údajů	37
9.3	Číselníky tarifních dat	37
10	Popis požadavků na zúčtovací centrum.....	38
11	Popis požadavků na datovou komunikaci (způsob distribuce dat)	40
11.1	Datové rozhraní pro distribuci whitelistů	40
11.2	Datová komunikace s externími systémy dopravců	40
11.3	Datová komunikace s mobilními zařízeními revizorů	41
12	Bezpečnostní požadavky na systém	43
12.1	Základní požadavky na návrh systému	43
12.2	Speciální požadavky na návrh systému	45
12.3	Základní požadavky na zabezpečení komunikace	46
12.4	Speciální požadavky na zabezpečení komunikace.....	46
13	Požadavky na mobilní aplikaci systému elektronického odbavení cestujících	49
14	Součinnost zadavatele	51
14.1	Odbavovací zařízení dopravců (strojky dopravců).....	51
14.2	MAP SAM moduly.....	54
14.3	Tokenizační mechanismus	55
14.4	Platební brána.....	56
14.5	Materiály a dokumentace pro nastavení systému zúčtování.....	56
14.6	Analýza k tvorbě QR kódu dle datové struktury MAP	57
14.7	ISIC	57
14.8	Využití přístupového bodu NIA.....	57
	Příloha č. 1 – Základní popis předpokládané implementace EOC ve VDV.....	58
	Příloha č. 2 – Požadavky na vytvoření tokenu z údajů získaných z identifikátorů systému EOC.....	59

1 Použité zkratky a pojmy

Bezkontaktní Karta (BK)	Identifikátor zákazníka v systému elektronického odbavení cestujících
Black list (BL)	Seznam zakázaných (karet nebo kupónů)
BPK	Bankovní platební karta
BČK	Bezkontaktní čipová karta dopravce
DESfire EV1	Standard/produkt bezkontaktní čipové karty, jehož dodavatelem je společnost NXP Semiconductors N.V.
DPMJ	Dopravní podnik města Jihlavy
EOC	Elektronické odbavení cestujících
Green list (GL)	Seznam změn ve White listu (increment WL)
HSM	Hardware Security Modul
IIN	Normalizované identifikační číslo vydavatelů karet
IK	In Karta ČD standardu MAP
JD	Jízdní doklad
KV	Kraj Vysočina
MAP	Technické řešení multiaplikační bezkontaktní čipové karty, jehož dodavatelem je společnost ODP-software s.r.o.
PAD	Příměstská autobusová doprava
Panmas	Zkrácené číslo BPK (Prvních 6 a poslední 4 pozice z čísla karty)
REST	Representational State Transfer
SAM	Secure access module, zařízení je určeno k bezpečnému uložení kryptografických klíčů a citlivých informací, vnitřní software tohoto zařízení poskytuje kryptografické a jiné funkce k zajištění bezpečných operací nad chráněnými daty
SOAP	Simple Object Access Protocol
SPP	Smluvní a přepravní podmínky

Taplist	Seznam přiložených karet (využívá se u BPK standardu EMV)
TOKEN	Jedinečný identifikátor bezkontaktní karty
VDV	Integrovaný dopravní systém Veřejné dopravy Vysočiny
White list (WL)	Seznam povolených záznamů (karet nebo kupónů)

2 Úvod

Cílem nově požadovaného systému je zajištění elektronického odbavení cestujících v integrovaném dopravním systému Veřejné dopravy Vysočiny (dále jen VDV). Primární funkcí tohoto systému je nákup dopravního produktu (například dlouhodobé předplatné, jednorázová jízdenka) a jeho přiřazení k libovolnému důvěryhodnému identifikátoru (například: bezkontaktní bankovní kartě, QR kódu v aplikaci mobilního telefonu, bezkontaktní paměťové čipové kartě standardu Mifare DESfire EV1 vydávané cizím subjektem).

Použitím libovolného důvěryhodného identifikátoru budeme pro účel tohoto dokumentu chápat přiřazení již zmiňovaného identifikátoru k zakoupenému produktu (jednorázové jízdence, dlouhodobému časovému kupónu apod.), tj. výsledkem výše uvedeného procesu bude vytvoření strukturovaného souboru dat „whitelistu“, který obsahuje informace o držiteli identifikátoru, zakoupených produktech, slevové kategorii cestujícího apod. Tento soubor dat bude dále použit pro vyhodnocení nároku na přepravu v IDS VDV.

V požadovaném řešení je kladen důraz na samoobslužné odbavení cestujícího. Systém musí obsahovat webový portál (webovou aplikaci) a mobilní aplikaci, která bude sloužit pro samoobslužné odbavení cestujícího, tj. uživatel systému realizuje veškeré činnosti (například: správu vlastního účtu a identifikátorů, nákup dopravního produktu apod.) prostřednictvím výše zmíněné webové a mobilní aplikace bez nutnosti návštěvy zákaznického centra dopravce. Vybudované řešení musí být univerzální a použitelné i pro dalšího zapojeného partnera (dopravce) v maximálně možné míře.

Součástí poptávky nejsou částečně již existující systémy, systémové komponenty a související služby a to zejména:

- Odbavovací zařízení ve vozidlech dopravců
- SAM moduly pro odbavovací zařízení
- Podklady a SW pro tokenizační mechanismus (zejm. klíč a dokumentace obsahující tokenizační vzorec),
- Platební brána pro elektronické platby bankovní platební kartou dle standardu EMV.

Parametry výše uvedených systémů, systémových komponentů a služeb jsou uvedeny níže v tomto dokumentu. Dodávka musí na tyto systémy navazovat.

3 Obecné požadavky

Řešením elektronického odbavení cestujících v integrovaném dopravním systému Veřejné dopravy Vysočiny se pro účel této části zadávací dokumentace rozumí:

1. **Vybudování systému elektronického odbavení cestujících dle požadavků, které jsou uvedeny níže v tomto dokumentu.**

Nově navržený systém musí naplňovat veškeré požadavky dané integrovaným tarifním Systémem Veřejné dopravy Vysočiny (jeho definice je popsána v Příloze č. 1).

2. **Zpracování projektové dokumentace jednotlivých částí systému v rozsahu:**

- Prováděcí projekt (popisující podrobný návrh řešení díla a jeho jednotlivých funkcí)
- Dokumentace skutečného provedení díla

3. **Zpracování Bezpečnostního projektu v rozsahu:**

- Bezpečnostní politika práce s tokeny v systému EOC VDV
- Způsob práce se SAM moduly
- Zabezpečení datové komunikace celého řešení
- Zabezpečení systému elektronického odbavení cestujících ve vztahu k dostupnosti, důvěrnosti a integrity dat
- Správu a řízení oprávnění uživatelů (obsluha zákaznického centra) systému elektronického odbavení cestujících
- Zabezpečení odbavovacích míst (zákaznická centra) systému elektronického odbavení cestujících

Poznámka

(Bezpečnostní projekt nově budovaného systému musí být zpracován ve vazbě na již existující bezpečnostní projekty Objednatele, které jsou tímto systémem dotčeny).

4. Předpokládaný harmonogram dodávky včetně stanovení hlavních milníků projektu

Etapizace	Název	Charakteristika	Předpoklad časové náročnosti (měsíce)
Etapa 0	Předprojektová příprava	• Příprava Zadávací dokumentace • Provedení předběžných tržních konzultací • Provedení zadávacího řízení veřejné zakázky • Uzavření smluvního vztahu s dodavatelem platební brány (bankou) • Uzavření (zveřejnění) smluvního vztahu s dodavatelem EOC (okamžik T0)	T0
Etapa 1	Projektování	• Zpracování a předání Prováděcího projektu • Schválení Prováděcího projektu • Příprava testovacího prostředí • Zajištění vybavení a součinnosti zadavatele • Zajištění vybavení a součinnosti dopravců	T0 až T0+3
Etapa 2	Vývoj a implementace	• Vývoj základního jádra zúčtovacího systému • Vývoj mobilní aplikace • Vývoj webové aplikace • Vývoj revizorského systému • Implementace zadané platební brány • Instalace HW a SW do prostředí Kraje Vysočina (zadavatele)	T0+3 až T0+11
Etapa 3	Testování	• Testování řešení dílčích částí systému dodavatelské testy • Beta testování u zadavatele • Pilotní provoz • Zahájení rutinního provozu • Předání aktualizovaného prováděcího projektu včetně dokumentace skutečného provedení díla	T0+11 až T0+13

Jako čas T0 je považován den uveřejnění smlouvy s dodavatelem v registru smluv

5. Integrace dodaného řešení do odbavovacího systému společnosti České dráhy a.s. – vzájemné uznávání identifikátorů cestujícího a výměnu seznamu zakázaných případně seznamu povolených karet.
6. Zaškolení pracovníků zadavatele pro užívání a správu systému
7. Návrh pravidel budoucího update a upgrade systému, včetně jeho profylaxe

8. **Návrh bližších servisních podmínek.** Po vzájemném odsouhlasení budou tyto bližší podmínky součástí servisní smlouvy.
9. **Dodání dokumentace systému – příručky obsluhy systému, příručka administrátora systému, technické výkresy a schémata řešení, dokumentace popisující možnosti a limity systému, postupů zálohování a obnovy systému apod.**
10. **Akceptace vybraných částí díla může být podmíněna úspěšným provedením penetračních testů u vybraných částí subsystému EOC. Penetrační testy budou provedeny 3. stranou a hrazeny objednatelem.**

Řešení projektu jako celek bude mít formu tří vrstvé architektury:

- Prezentační vrstva (například: e-shop, aplikace pro správu systému, mobilní aplikace)
- Aplikační vrstva – vlastní funkce/logika systému
- Datová vrstva (databáze osobních dat uživatelů systému a jejich identifikátorů, databáze prodejních transakcí, databáze číselníků a tarifních dat)

Požadavky kladené na systém EOC VDV:

- Systém bude dimenzován pro minimálně 500.000 uživatelů
- Systém bude dále dimenzován pro minimálně 9.5 milionu prodejních transakcí za kalendářní rok
- Řešení musí umožnit zapojení minimálně 50 odbavovacích přepážek dopravců (jedná se o kontaktní místo určené pro odbavení klienta, vyřizování reklamací apod.)
- Dostupnost systému dle SLA
- Systém bude provozován v geograficky oddělených lokalitách
- Data systému budou pravidelně zálohována
- Rozhraní pro předávání dat (například: strukturovaných souborů pro odbavovací zařízení ve voze dopravce) bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy. Je však nutné dodržet vysoké bezpečnostní standardy tohoto řešení.

- Veškerá datová komunikace bude šifrovaná
- Osobní údaje budou v databázi uchovávány v šifrované podobě s oddělením identifikátorů a osobních údajů
- Zadavatel požaduje instalaci a provozování nově vybudovaného systému ve vlastním serverovém prostředí (tj. hardwarovém, softwarovém a síťovém prostředí).
- Zadavatel požaduje spolupráci systému EOC s API rozhraním do DB ISICu pro on-line ověřování studentských průkazů při prvotní registraci identifikátoru cestujícího v systému EOC. Pro odladění služby je k dispozici testovací DB dostupná na webu vydavatele ISIC.
- Systém EOC VDV bude získávat data o transakcích mimo jiné propojením s Back-office dopravců
- Zadavatel předpokládá budoucí vzájemné uznávání jízdních dokladů s okolními IDS.

Požadavky na komunikaci EOC se strojky dopravců

Zadavatel požaduje otevřenost dodávaného řešení k budoucím změnám spočívajícím v přímé komunikaci EOC s odbavovacími strojky ve vozidlech.

Předpokládané kapacity Technologického centra KV:

Řešení bude provozováno v Technologickém centru Kraje Vysočina v prostředí serverové virtualizace (farma Vmware vSphere Enterprise verze 7+) typicky na serverové platformě MS Windows 2019.

Předpokládaný výkon alokovaný z fyzických hostů všemi virtuálními stroji (cca 6 kusů VM, celkem max 24 vCPU,) je 6 GHz CPU, max. spotřeba paměti RAM je 100 GB, disková storage SSD max 1TB, NLSAS max 10TB.

Akceptovatelné operační systémy na virtuálních strojích budou:

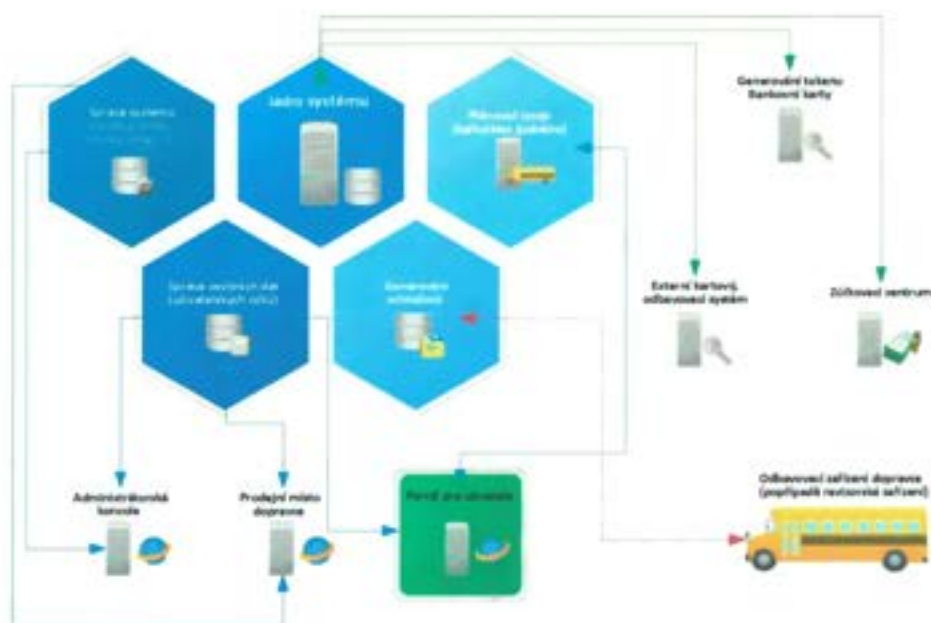
- MS Windows 2019
- GNU/Linux Debian (v době implementace stabilní verze)
- GNU/Linux Red Hat Enterprise Linux (Full-support subscription na 5 let a maintenance support subscription na dalších 5 let zajišťuje dodavatel)

K dispozici jsou mechanismy vysoké dostupnosti (HA režim VMW), síťové ochrany VMWAre NSX, Web Application Firewallu (F5 BIG IP) a zálohování je zajištěno nativními nástroji použité serverové virtualizace, systémem Veeam.

Licence OS Microsoft Windows Server Datacenter a sdíleného MS SQL 2019 Standard serveru jsou zajištěny zadavatelem.

Zhotovitel je povinen Zadavateli předložit požadavky na zajištění odpovídající a přiměřené serverové části na provozování systému elektronického odbavení cestujících.

Základní požadavky na architekturu systému:



Požadavky na systém elektronického odbavení cestujících shrnuje výše uvedené schéma.

Jádro systému

Základní prvek systému, zajišťující vlastní aplikační logiku celého systému, musí plnit minimálně tyto funkce:

- Výpočet jízdného (stanovení ceny za produkt)
- Správa životního cyklu uživatele systému EOC VDV
- Správu životního cyklu karty a ostatních identifikátorů EOC VDV

- Správu tarifní politiky integrovaného dopravního systému VDV
- Generování strukturovaných souborů – whitelistů
- Komunikaci s externími systémy při procesu ověřování Identifikátorů EOC VDV
- Generování jedinečných identifikátorů
- Integraci s platebními metodami (e-Commerce platební brána, automatizované zpracování převodních příkazů)
- Komunikaci s externími kartovými a odbavovacími systémy při procesu prodeje dopravního produktu pro uživatele systému
- Příprava a distribuce dat pro zúčtovací systém

Správa systému

musí zajišťovat minimálně následující funkce:

- Správu subjektů a dopravců zapojených do systému
- Definici a správu jednotlivých číselníků (typy identifikátorů, zákaznické kategorie, tarify, zóny, ceníky pro jednotlivé tarify, trasy a linky, zastávky, účetní položky, sazby DPH apod.)
- Administrace jednotlivých dopravních produktů dle tarifní politiky VDV (včetně parametrů, které jsou nutné k realizaci prodeje dopravního produktu)

Správa osobních dat

musí zajistit minimálně následující funkce:

- Bezpečné uchování osobních dat uživatelů systému (archiv osobních údajů)
- Realizovat změnové požadavky při správě osobních údajů (změna jména, příjmení, fotografie apod.)

Ostatní části systému

požadavky na ostatní části systému jsou dále podrobně popsány v jednotlivých kapitolách:

- Portál zákazníka, e-shop – uvedeno v kapitole 5
- Administrátorská konzole – uvedeno v kapitole 6
- Prodejní místo u dopravce (SW)– uvedeno v kapitole 7
- Požadavky na systém mobilních zařízení pro revizory – uvedeno v kapitole 8
- Generování whitelistu – uvedeno v kapitole 9
- Zúčtovací centrum – uvedeno v kapitole 10
- Popis požadavků na rozhraní systému (kalkulátor jízdného, napojení na externí odbavovací systémy) – uvedeno v kapitole 11

4 Typy identifikátorů v systému EOC

4.1 Bezkontaktní bankovní karta

Jedná se o jeden z možných identifikátorů zákazníka v systému elektronického odbavení cestujících. Z důvodu komfortního a rychlého odbavení držitele karty v odbavovacím zařízení ve voze veřejné dopravy budou v systému využity pouze bankovní karty bezkontaktní.

Odbavení karet v odbavovacím zařízení ve vozech veřejné dopravy/platebním terminálu bude řešeno v tzv. *off-line režimu*. Zadavatel požaduje, aby odbavení cestujícího nevyžadovalo potvrzení PINem.

Bankovní karty, které budou integrovány do nově budovaného systému:

- Bezkontaktní bankovní karta (možno použít také hybridní bankovní karty obsahující: magnetický proužek, kontaktní a bezkontaktní čip)
- Kreditní, debetní a předplacená bankovní karta vydaná asociací Mastercard, VISA (popřípadě další: Diners Club)
- Bankovní karta vydaná ve formě „mezinárodní karty“ (mezinárodně akceptované bankovní karty) nebo „domácí karty“ (bankovní karty akceptované pouze na území České republiky)

Požadavky na získání jedinečného identifikátoru (tokenu) z bezkontaktní bankovní karty:

V systému elektronického odbavení cestujících bude využita pouze identifikační funkce karty, tj. z vyčtených údajů z bankovní karty bude vytvořen unikátní identifikátor. Z takto vytvořeného identifikátoru nebude možné standardním způsobem zpětně zjistit zdrojová data získaná z bankovní karty.

Jedinečný identifikátor – Token bude počítat pouze platební brána, **proces tokenizace BPK tedy není součástí poptávaného systému.**

4.2 QR kód generovaný mobilní aplikací

Další možností vytvoření jedinečného identifikátoru v systému EOC bude vygenerování tohoto identifikátoru prostřednictvím mobilní aplikace.

Zadavatel disponuje analýzou a návrhem struktury QR kódu včetně podrobného popisu doporučené datové struktury MAP- viz. kap. 14.6 Podrobný popis návrhu datové věty bude předán zhotoviteli nejpozději v průběhu přípravy Cílového konceptu.

Identifikátor typu QR kód bude jedinečný pro každou jednotlivou instalaci mobilní aplikace v telefonu i v rámci jednoho uživatelského účtu (z uvedeného vychází i požadavek na unikátnost v rámci instalace do různých mobilních zařízení)

Prezentace identifikátoru bude v mobilní aplikaci realizována prostřednictvím 2D čárového kódu (QR kód). Takto generovaný kód musí být zabezpečen možností ověření získaných dat.

Mobilní aplikace, která bude tento QR čárový kód zobrazovat musí zajistit ochranu proti vytvoření tzv. snímku obrazovky.

Zadavatel požaduje, aby realizace systému umožňovala případné budoucí použití dynamického QR kódu ve smyslu nahrazení statického QR kódu.

Požadavky na získání jedinečného identifikátoru (tokenu) z QR kódu mobilní aplikace:

- Jedinečný identifikátor (token) bude počítán při registraci QR kódu do systému EOC speciální službou back office EOC. Pro zabezpečení funkce odbavení bude ve vozidlech k dispozici SAM. Bude použit speciální algoritmus pro identifikátory, typu QR kód a BČK.
- Identifikátor(-y) bude(budou) automaticky přiřazen(-y) k účtu uživatele (pro možnost nákupu a přiřazení dopravního produktu)

Systém elektronického odbavení cestujících musí zajistit rozlišení tohoto typu identifikátoru.

4.3 Bezkontaktní čipové karty vydávané dopravcem

Hlavním požadavkem této funkcionality je využití existujících dopravních karet (bezkontaktních čipových karet) jejichž vydavateli jsou subjekty poskytující veřejnou dopravu na území IDS VDV.

Dopravní karty, které budou integrovány do nově budovaného systému:

- In Karta (nový typ karty typu/standardu MAP)
 - Vydavatelem je společnost České dráhy a.s.
 - Technologie: DESfire EV1 8kB
 - Rozlišení nového typu karty: symbol MAP ready (grafický prvek vytištěný na kartě)
 - Typ vydávané karty: personalizovaná a nepersonalizovaná karta (pro registrované uživatele dle kap 5.2)
 - Dále lze karty rozlišit dle použití: zákaznická karta (personalizovaná), služební karta (personalizovaná), business karta (nepersonalizovaná karta)
 - Karta je vydávána s platností 5 let
 - Identifikační údaje na kartě (personalizované): Jméno, příjmení, datum narození, fotografie držitele karty, unikátní číslo vydané karty a platnost karty
- Jihlavská karta

- Vydavatelem je společnost Dopravní podnik města Jihlavy, a.s.,
- Technologie: DESfire 4kB
- Typ vydávané karty: personalizovaná a nepersonalizovaná karta
- Karta je vydávána s platností 4 roky
- Identifikační údaje na kartě (personalizované): Jméno, příjmení, fotografie držitele karty, unikátní číslo vydané karty

Požadavky na získání jedinečného identifikátoru (tokenu) z IN Karty:

Registrace karty do systému bude realizována na základě vyplnění unikátního čísla karty (18-místné číslo karty definované dle ISO/IEC 7812-1, postup přidělování tohoto čísla pak normou ISO/IEC 7812-2) a platnosti karty (oba údaje jsou vytištěny na kartě).

- Systém následně ověří platnost zadaného čísla karty za použití metody Luhnův algoritmus (tj. shoda výpočtu s kontrolní číslicí 18. pozice v čísle karty). Dále ověří, zda je karta platná.
- Systém dále ověří zadané číslo karty oproti seznamu zakázaných karet
- Po vyhodnocení výše uvedených dat bude vygenerován jednoznačný identifikátor – Token (obdobným způsobem, který je uveden v případě QR kódu). Tedy:
- Jedinečný identifikátor (token) bude počítán při registraci IN Karty do systému EOC speciální službou back office EOC. Pro zabezpečení funkce odbavení bude ve vozidlech k dispozici SAM. Bude použit speciální algoritmus pro identifikátory, typu QR kód a BČK.
- Popis tokenizačního mechanismu je uveden v příloze č.2.

Požadavky na získání jedinečného identifikátoru (tokenu) z Jihlavské karty:

Zadavatel požaduje implementovat funkci dle následujícího popisu:

- Registrace karty do systému bude realizována na základě vyplnění unikátního čísla karty, případně iniciálu jména, příjmení držitele karty.
- Pro výpočet vstupních dat do tokenizačního algoritmu bude využito pouze UID karty (resp. číslo Jihlavské karty)
- Systém následně prostřednictvím externí webové služby ověří platnost zadaného čísla karty. Externí webová služba poskytne vstupní data pro vygenerování jednoznačného identifikátoru. Zadavatel v současnosti jedná s vydavatelem Jihlavské karty na budoucím zprovoznění tohoto postupu ověřování
- Jedinečný identifikátor (token) bude počítán při registraci Jihlavské karty do systému EOC speciální službou back office EOC. Pro zabezpečení funkce odbavení bude ve vozidlech k dispozici SAM. Bude použit speciální algoritmus pro identifikátory typu QR kód a BČK.
- Popis tokenizačního mechanismu je uveden v příloze č. 2

Alternativa k tokenizaci identifikátorů typu QR kód a BČK

Zadavatel nevylučuje použití alternativního způsobu identifikace cestujícího v systému EOC a to pouze použitím vstupních dat (číslo karty, expirace, číslo QR kódu). Vše za předpokladu dodržení všech bezpečnostních standardů.

Zapojení karet dalších dopravců do systému EOC VDV

Systém musí být navržen tak, aby umožňoval budoucí zapojení dalších dopravců, u kterých mohou být použity odbavovací technologie využívající karty Mifare Desfire (Mifare Desfire EV1). Systém má být připravený pro rozšíření o funkci akceptace dalších typů identifikátorů.

5 Požadavky na samoobslužný systém pro odbavení zákazníků (portál zákazníka, e-shop)

5.1 Základní funkce

Tuto část systému je nutné navrhnout formou webové aplikace. Z pohledu bezpečnosti je nutné použití zabezpečené komunikace se severem prostřednictvím https protokolu.

Webová aplikace musí být vytvořena principem responzivního designu webu (tj. aplikaci bude možné „použít“ i v mobilním telefonu, tabletu apod.) Aplikace musí být použitelná v běžně rozšířených internetových prohlížečích.

Základní požadavky kladené na samoobslužný systém odbavení zákazníků (portál zákazníka, e-shop):

- Založení a správa uživatelského účtu zákazníka (vč. podúčtů celého platebního systému)
- Funkce registrace (přiřazení jednoznačného identifikátoru k účtu uživatele)
- Správu identifikátorů
- Správa zakoupených produktů
- Správa zákaznických profilů/kategorií
- Nákup a úhrada dopravního produktu
- Systém musí umožňovat budoucí rozšíření o funkci automatické registrace a autentizace prostřednictvím elektronické identity s úrovní záruky střední a vysoká dle zákona 250/2017 Sb. o elektronické identifikaci (např. elektronickým Občanským průkazem)
- Portál zákazníka, e-shop bude integrován do webového portálu VDV

Zadavatel požaduje otevřenost portálu zákazníka k budoucímu propojení s datovým rozhraním aplikace pro veřejnost Centrálního dispečinku VDV.

5.2 Životní cyklus uživatele systému

Každý uživatel (cestující), který bude evidován v systému EOC, musí být zařazen do jedné z níže uvedených kategorií:

Definice kategorie uživatele

- **Uživatel registrovaný**, došlo k vyplnění a následnému ověření přihlašovacích údajů v rozsahu: jméno (emailová adresa uživatele) a heslo
- **Uživatel personalizovaný**, došlo k vyplnění osobních údajů, minimálně v tomto rozsahu:
 - Jméno a příjmení
 - Datum narození
 - Bydliště
 - Fotografie (rozměr průkazové fotografie, systém musí ověřovat formát a kvalitu vloženého souboru)
 - V případě uživatele, který ještě nedosáhl věku 15 let, bude nutné doplnit i osobní údaje zákonného zástupce
- **Uživatel s platným účtem**, došlo k ověření osobních údajů klienta (například prostřednictvím kontaktního místa, automatických procesem apod.)

Pokud se uživatel systému rozhodne upravit vlastní osobní údaje (například jméno, příjmení nebo fotografii), které již byly ověřeny, tak bude nutné tento stav identifikovat a zamezit neoprávněné manipulaci s účtem, tj. stav přesunout do „nižší“ kategorie – Uživatel personalizovaný.

Každý z výše uvedených stavů musí být v systému zohledněn v podobě rozsahu nabízených služeb (například: registrovaný (anonymní) uživatel nebude mít možnost nákupu nepřenositelného typu dopravního produktu, naopak uživatel s platným účtem bude mít možnost nákupu také přenosných typů dopravních produktů.

Definice zákaznického (uživatelského) profilu cestujícího

Zákaznickým profilem budeme pro účel tohoto dokumentu chápat identifikaci slevové (nebo jiné) kategorie, která je uživateli systému (držiteli karty) přiznána na základě pravidel uvedených ve Smluvních přepravních podmínkách VDV. Dále je možné výše uvedené označit *jen zkratkou CP „Customer Profile“*. Vlastní číselník zákaznických profilů vychází z EN 1545-1.

5.3 Správa uživatelského profilu cestujícího

Z pohledu prokázání nároku na nákup daného typu dopravního produktu je nutné uživateli systému přiřadit tzv. uživatelský profil (například: dospělý, dítě, student, důchodce, ZTP apod.).

Způsoby přiřazení uživatelského profilu:

- Automaticky přiřazen (například uživatelský profil – dospělý)
- Přiřazen na základě správcem systému schválené žádosti podané ze strany uživatele systému

Portál pro uživatele musí zajistit možnost podání žádosti o přiřazení uživatelského profilu (žádost bude uživateli systému automaticky nabídnuta v případě splnění věkového nebo jiného omezení pro daný profil). Vlastní proces schválení žádosti již bude probíhat v části systému „Prodejní místo“.

5.4 Registrace identifikátorů

Uživateli systému (bez ohledu na kategorii uživatele) bude umožněno přiřazení libovolného počtu nabízených typů identifikátorů.

Uživateli systému musí být umožněno realizovat zablokování identifikátoru v případě jeho ztráty, krádeže apod.

Podrobný popis výpočtu jedinečného identifikátoru (tokenu) při registraci identifikátoru v systému je uveden v příloze č. 2

5.5 Výběr a úhrada produktu

Systém musí zajistit výběr dopravních produktů dle tří níže uvedených postupů.

5.5.1 Výběr dle tarifu

Uživateli systému bude umožněn nákup dopravního produktu dle aktuálně přiřazeného zákaznického (uživatelského) profilu, tj. bude zobrazena nabídka všech tarifů, které se vážou k profilu uživatele. Na základě realizovaného výběru tarifu bude uživateli dále nabídnuto období platnosti a možnost výběru územní platnosti.

5.5.2 Výběr pomocí kalkulatoru jízdného

Uživateli systému bude umožněn nákup dopravního produktu, jehož definici určí na základě zvolené trasy, přiřazeného zákaznického profilu a období platnosti. Na základě zpracování tohoto požadavku datovým rozhraním „Kalkulator jízdného“ bude uživateli nabídnut nejvhodnější produkt včetně stanovení jeho ceny v tarifu VDV. Zadavatel požaduje dodat popisované řešení jako součást e-shopu a mobilní aplikace.

5.5.3 Výběr pomocí vyhledávače spojení

Uživateli systému bude umožněn výběr vhodného spojení (zvolené trasy) pomocí vyhledávače spojení. Řešení musí být navrženo tak, aby bylo možné na základě zvolených začátečních a koncových stanic cesty, zákaznického profilu a období platnosti nabídnout uživateli nákup nejvhodnějšího dopravního produktu v tarifu VDV. Zadavatel požaduje dodat popisované řešení jako součást e-shopu a mobilní aplikace.

Vlastní úhrada za produkt bude řešena formou:

- On-line transakce prostřednictvím platební brány
- Převodním příkazem (a následným automatickým párováním platby, tj. zpracováním datových souborů avíz získaných z rozhraní banky). Platební informace (potvrzení o platbě) bude zaslána uživateli na email, který uvedl při založení účtu. Zadavatel požaduje garanci úhrady jízdného dokladu před zahájením jeho platnosti (např. Dokončení nákupu bude podmíněno odesláním převodního příkazu)

Zjednodušený daňový doklad o realizované úhradě dopravního produktu bude uživateli zaslán na email, který uvedl při založení účtu.

5.6 Správa zakoupených produktů

Uživateli systému musí být umožněno zobrazení transakční historie zakoupených (platných/neplatných) dopravních produktů.

Transakční historie musí obsahovat minimálně:

- Stav produktu (platný/neplatný, stornováno, neuhrazeno apod.)
- Typ produktu
- Časová platnost
- Územní platnost
- Zákaznický profil
- Datum a čas pořízení produktu, datum a čas úhrady produktu
- Typ platební metody

Uživateli systému bude dále umožněno:

- Požádat o storno produktu (jehož platnost nebyla zahájena), nebo o přerušení aktuálně platného produktu. Vlastní proces vyřízení této žádosti musí být následně realizován prostřednictvím pracovníka obsluhy systému v části „Prodejní místo“
- Přearadit aktuálně platný produkt (popřípadě platný v budoucnosti) na libovolný typ zaregistrovaného a platného identifikátoru v účtu uživatele. Tento proces nebude možno realizovat s okamžitou účinností z důvodu času nutného pro vygenerování a distribuci whitelistu do akceptačních zařízení dopravců.

6 Požadavky na systém administrace

6.1 Základní funkce

Administrátorská část systému bude určena pro základní definici hodnot nutných pro správu subjektů a dopravců zapojených do systému, dále musí zajistit možnost stanovení tarifních ukazatelů nutných pro vytvoření dopravního produktu určeného k prodeji prostřednictvím e-shop zákaznického portálu. Minimální požadavky na administraci celého systému jsou uvedeny níže v jednotlivých bodech.

6.2 Správa subjektů a dopravců

Pro každý partnerský subjekt nebo každého dopravce, který je zapojen do systému EOC musí existovat záznam určující rozsah jeho oprávnění k vykonávání jednotlivých funkcí systému (prodej dopravního produktu, ověřování osobních dat uživatelů, právo schválení zákaznické kategorie apod.).

Oprávnění každého subjektu nebo každého dopravce musí v systému definovat:

- Samostatná skupina oprávnění pro obsluhu systému

Pro každý subjekt nebo každého dopravce musí být v systému vytvořeny minimálně tyto funkcionality:

- Samostatná evidence prodeje dopravních produktů
- Účetní a statistický reporting vázaný k danému subjektu/dopravci
- Samostatné generování a distribuce dat do zúčtovacího centra

6.3 Správa číselníků

Pro vlastní definici jednotlivých dopravních produktů/tarifů bude nutné v systému umožnit správu vstupních dat. (tyto data určují parametry pro nabízení a prodej dopravních produktů, popřípadě definují vazby mezi těmito parametry).

Systém musí obsahovat správu minimálně těchto číselníků:

- Dopravní produkt/Tarif bude obsahovat minimálně atributy:
 - Identifikace tarifu
 - Slovní označení tarifu

- Typ tarifu (definice časové období určující jeho platnost, například na pevný počet dnů, volitelný počet dnů apod.)
- Příslušnost ke kategorii cestujících
- Vazbu na územní platnost (definice dle zónově relačního tarifu)
- Propojení na ceník
- Definice parametrů určující vlastní nabízení a prodej dopravního produktu
- Ceník dopravního produktu/Tarifu bude obsahovat minimálně atributy:
 - Identifikaci ceníku
 - Platnost ceníku
 - Účinnost ceníku
- Kategorie cestujících bude obsahovat minimálně atributy:
 - Identifikátor kategorie cestujících (číselník musí vycházet z EN 1545-1)
 - Slovní označení kategorie cestujících
 - Platnost kategorie cestujících
 - Definice nároku dle věkového omezení
 - Vazbu na stav účtu uživatele
- Definice zóny bude obsahovat minimálně atributy:
 - Identifikace zóny
 - Slovní označení zóny
 - Vazba na nadzóny
 - Počet tarifních jednic v zóně
 - Vazba na hraniční zastávky/referenční zastávku v zóně

- Definice nadzóny bude obsahovat minimálně atributy:
 - Identifikace nadzóny
 - Slovní označení nadzóny
- Číselník zastávek
- Číselník linek/spojů
 - Možnost definice povolené trasy v rámci výčtu zón
- Číselník typů dokladů (příjmový, výdajový, reklamační apod. včetně definice číselných řad)
- Číselník sazeb DPH

6.4 Správa tarifu

Tato část systému musí zajistit vlastní sestavení/definici dopravního produktu dle zvolených hodnot vycházejících z výše uvedených číselníků (například určením vazby mezi tarifem, kategorií cestujícího, definicí územní platnosti a ceníkem).

Nově navrhovaný tarif bude možné přiřadit k využití (nabízení k prodeji) u definovaného subjektu, popřípadě konkrétně specifikovaného prodejního místa.

6.5 Správa subjektů a dopravců jako uživatelů systému

Oprávnění každého subjektu nebo každého dopravce musí v systému definovat samostatná skupina oprávnění pro přístup do systému. Uživatelské přístupy do systému se budou realizovat prostřednictvím rolí, které definují oprávnění k jednotlivým funkcionalitám systému (tj. podle povahy činnosti uživatele v systému).

Základní uživatelské role a příslušná oprávnění jsou následující:

- Administrátor systému
- Správce subjektu
- Pracovník prodejního místa

- Správce prodejního místa
- Pracovník informační přepážky

Každou roli bude možné přiřadit/definovat samostatně pro konkrétní subjekt/dopravce zapojeného do systému.

Ověření uživatelů systému

Uvedené způsoby ověření včetně využití IDM se týkají pouze vnitřních uživatelů systému EOC (účet správce systému, účet pracovníků prodejních míst apod.) a netýkají se public users (cestujících).

Požadované způsoby ověření:

- Autentizace (ověření uživatele) k webovému (tenkému) klientovi prostřednictvím SSO Kraje Vysočina (SAML2) federace VysočinaID viz <https://vysocinaid.kr-vysocina.cz/>
- Autentizace k windows (těžkému) klientovi prostřednictvím autentizační služby IDM Kraje Vysočina nebo pomocí LDAP(S) (MS Active Directory) dle konkrétních potřeb implementace a možností zadavatele.

Využití Identity managementu KV

Pro získání oprávnění uživatelů a jejich metadat (autorizace) bude využit Identity management KV (IDM AC Identita). IDM má vystaveno aplikační rozhraní (API) ve formě web služeb SOAP (WS). Aplikace získává profil daného uživatele včetně oprávnění (rolí) prostřednictvím API na IDM KV, ukládá tyto parametry do svého interního nástroje správy uživatelů a v proceduře autorizace přiděluje na základě úspěšné autorizace příslušná oprávnění. V aplikaci budou vytvořené 2 tabulky, které budou obsahovat data o prováděných synchronizacích mezi aplikací a API IDM. První tabulka bude souhrnná a bude obsahovat záznamy o provedených synchronizacích (id, začátek synchronizace, konec synchronizace, stav (OK, Error), druhá tabulka bude detailová a bude obsahovat změněné záznamy v rámci dané synchronizace (ID, ID_synchronizace, změna, stav (Ok, Error)). Dané tabulky budou sloužit k napojení na monitorovací systém Kraje Vysočina (PRTG) a jejich přesnou definici poskytne zadavatel v rámci implementace, výše uvedené hodnoty jsou pouze demonstrativní.

6.6 Správa prodejních míst

Nabídka a prodej dopravních produktů bude (mimo jiné) prováděn prostřednictvím dvou hlavních prodejních kanálů systému. E-shopu zákazníka (portálu zákazníka) a prodejního místa dopravce.

Každý subjekt/dopravce zapojený do systému bude mít definován vlastní seznam prodejních míst (například z důvodu rozlišení prodejních míst do logických celků). Uvedené členění bude realizováno i z důvodu účetní evidence transakcí (prodeje produktů koncovým zákazníkům) za jednotlivá prodejní místa subjektu/dopravce a přípravy dat pro zúčtování prostřednictvím zúčtovacího centra, tj. prodejní místa je nutné označit jednoznačným identifikátorem v rámci daného subjektu/dopravce včetně vlastní transakční/dokladové číselné řady.

U každého dopravního produktu bude možné určit jeho vazbu k prodejnímu místu.

6.7 Správa sestav

Systém musí zajistit generování účetních a statistických sestav minimálně v níže uvedeném rozsahu:

- Účetní uzávěrky (souhrn prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu). Sestava musí obsahovat sumu za prodej/storno dle jednotlivého typu produktu, platební metody, uživatele/prodejního místa/subjektu).
- Seznam všech prodejních transakcí (přehled prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu)
- Seznam všech objednávek produktů prostřednictvím e-shop (přehled objednávek, dle definovaného období, typu produktu, platební metody, stavu objednávky /zaplaceno, čeká na zaplacení z platební brány, stornováno apod./)
- Statistická sestava počtu prodaných dopravních produktů dle jednotlivého tarifu a zákaznické kategorie (přehled minimálně dle definovaného období)
- Statistická sestava o počtu evidovaných identifikátorů v systému z pohledu jejich platnosti platný/blokovaný/vyřazený z důvodu překročení platnosti (přehled minimálně dle definovaného období)
- Statistická sestava o počtu evidovaných identifikátorů v systému dle typu bankovní karta/2D kód/dopravní karta (přehled minimálně dle definovaného období)
- Statistická sestava o počtu registrovaných uživatelů v systému z pohledu stavu účtu (přehled minimálně dle definovaného období)

- Statistická sestava – demografická data o uživateli systému (přehled minimálně dle definovaného období)

Systém dále umožní generování vlastních uživatelských sestav na základě dostupných nástrojů „generátorů sestav“ (v rámci přípravy Prováděcího projektu budou stanoveny/popsány datové matice určené pro využití v generátoru sestav).

7 Požadavky na prodejní portál (prodejní místo –předprodej u dopravce)

Požadovaný způsob pro návrh aplikace prodejního místa (prodejního portálu)

Portál je určen pro využívání na počítačích dopravců, na pokladních předprodejních místech dopravců. Portál bude vytvořen prostřednictvím webové aplikace, která bude přístupná ze sítě Internet na základě definovaného/povoleného rozsahu IP adres. Z pohledu bezpečnosti bude nutné využití zabezpečené komunikace se serverem prostřednictvím https protokolu. Přístupová oprávnění k aplikaci budou řešena na úrovni Administrátorské části systému. Navržené řešení musí zajistit zprovoznění prodejního místa u dopravce bez velkých nároků na hardwarové a softwarové vybavení. Součástí vybavení prodejního místa, které si zajistí ve vlastní režii jednotliví dopravci, bude tiskárna pro tisk prodejních dokladů, zařízení pro skenování dokladů a fotografií cestujících, čtečky identifikátorů EOC, platební terminál pro BPK. Zhotovitel EOC pouze vypracuje návrh HW konfigurace.

Zadavatel požaduje možnost propojení systému EOC s portálem VDV webu Kraje Vysočina), u něhož předpokládá, že dlouhodobě zůstane pro cestujícího hlavním přístupovým bodem.

7.1 Požadované funkcionality prodejního portálu

Obsluha portálu bude umožněna (dle typu oprávnění) minimálně:

- Vyhledání detailu uživatele (s možností definice filtru: jméno, příjmení; uživatelské jméno)
- Úprava osobních dat uživatele včetně pořízení (například webovou kamerou apod.) a výměny fotografie
- Zrušení účtu
- Vytvoření dodatečných údajů k účtu uživatele (například formou poznámky)
- Založení a správa uživatelského účtu

7.2 Ověřování uživatele (cestujícího)

Obsluha portálu bude zajišťovat ověřování osobních dat uživatelů systému (například ověřením prostřednictvím občanského průkazu) a na základě tohoto úkonu bude umožněno přepnutí účtu do stavu popsaného v kapitole 5.2.

7.3 Správa identifikátorů uživatele (cestujícího)

Obsluha portálu bude umožněna správa identifikátoru (m.j. bezkontaktní bankovní karty a dopravní karty) přiřazeného k účtu uživatele. Jedná se o blokování a odstranění identifikátoru.

7.4 Správa zákaznických (uživatelských) profilů cestujících

Obsluha portálu bude:

- na přepážce fyzicky přijímat žádosti o přiřazení uživatelského profilu k účtu uživatele
- ověřovat a schvalovat žádosti o přiřazení uživatelského profilu k účtu uživatele (včetně žádostí vzniklých na straně uživatele systému dle kapitoly 5.3.).

V případě schválení žádosti (předložení požadovaných dokladů dle pravidel SPP VDV) o zákaznickou kategorii bude obsluha systému definovat pouze období platnosti uvedené kategorie (profilu).

V systému musí být umožněno přiřazení uživatelského profilu (zákaznické kategorie) k účtu i bez odeslání žádosti ze strany uživatele. Například uživatelský profil – dospělý bude přiřazen automaticky.

7.5 Prodej dopravních produktů

Úhrada za produkt bude řešena formou:

- Hotovostní úhrady
- Bezhotovostní úhrady prostřednictvím platebního terminálu

Zjednodušený daňový doklad o realizované úhradě dopravního produktu bude uživateli zaslán buď na email, který uvedl při založení účtu, nebo bude vytištěn na pokladní tiskárně.

Systém musí zajistit prodej dopravních produktů dle níže uvedených postupů:

- Výběr produktu dle tarifu

Obsluze portálu bude umožněn prodej dopravního produktu dle aktuálně přiřazeného uživatelského profilu (zákaznické kategorie) daného uživatele (tj. bude zobrazena nabídka všech tarifů, které se vážou k zákaznické kategorii uživatele). Na základě realizovaného výběru tarifu bude Obsluze dále nabídnuto časové období platnosti a možnost výběru územní platnosti.

- Výběr produktu pomocí kalkulatoru jízdného

Obsluze portálu bude umožněn prodej dopravního produktu, jehož definici určí na základě zvolené trasy, výběru aktuálně přiřazené zákaznické kategorie (uživatelského profilu) zvoleného uživatele a období platnosti. Na základě zpracování tohoto požadavku datovým rozhraním „Kalkulátoru jízdného“ bude Obsluze nabídnut nejvhodnější produkt včetně stanovení jeho ceny.

- Výběr pomocí vyhledávače spojení

Obsluze portálu bude umožněn výběr vhodného spojení (zvolené trasy) pomocí vyhledávače spojení. Řešení musí být navrženo tak, aby bylo možné na základě zvolených začátečních a koncových stanic cesty, zákaznického profilu a období platnosti nabídnout uživateli nákup nejvhodnějšího dopravního produktu v tarifu VDV.

7.6 Prodej doplňkových produktů

Portál bude zajišťovat i prodej produktů, které nesouvisí s odbavením ve veřejné dopravě (například reklamních předmětů, obalů na kartu apod.).

Vlastní definice těchto produktů bude spravována v Administrátorské části systému.

Úhrada za produkt bude řešena formou:

- Hotovostní úhrady
- Bezhotovostní úhrady prostřednictvím platebního terminálu

Zjednodušený daňový doklad o realizované úhradě doplňkového produktu bude uživateli zaslán buď na email, který uvedl při založení účtu, nebo bude vytištěn na pokladní tiskárně.

7.7 Účetní a statistické sestavy

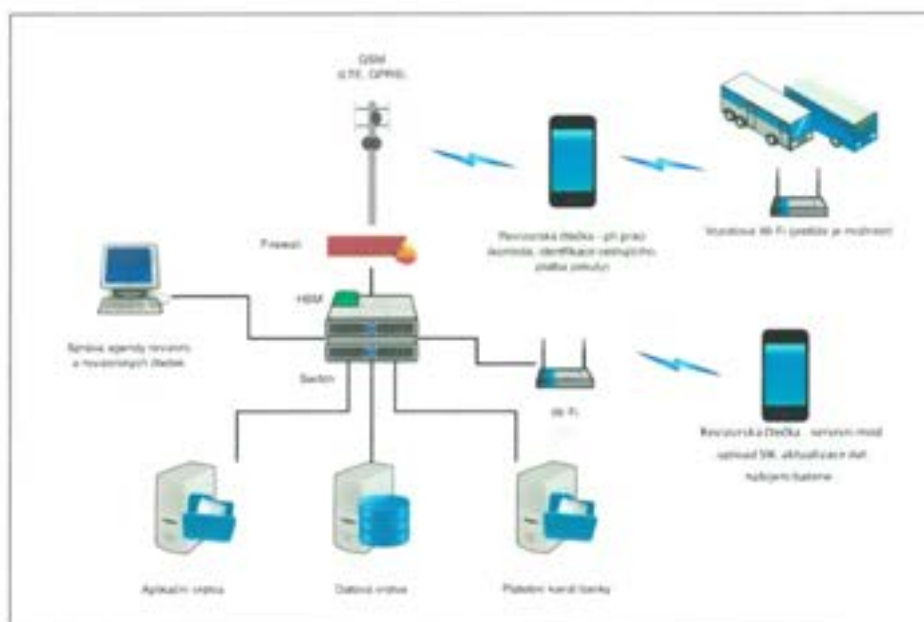
Portál musí zajistit generování účetních a statistických sestav pro pracovníka obsluhy minimálně v níže uvedeném rozsahu:

- Účetní uzávěrky (souhrn prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu). Sestava musí obsahovat sumu za prodej/storno dle jednotlivého typu produktu, platební metody, uživatele/prodejního místa/subjektu).

- Seznam všech prodejních transakcí (přehled prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu)

8 Požadavky na systém mobilních zařízení pro revizory

Architektura a celková funkce systému mobilních čteček



Požadované funkce systému:

Poptávané mobilní čtečky musí být schopny rutinního provozování následujících funkcí:

- Kontroly identifikátorů cestujícího v předpokládaných podobách:
 - karta dopravců Mifare DESfire (Mifare Desfire EV1)
 - bezkontaktní bankovní karta
 - QR kód na displeji mobilního zařízení cestujícího
- Zadavatel požaduje nepoužívat virtuální SAM moduly
- Kontroly jednorázového jízdného (zakoupeného v papírové podobě, nebo přes mobilní aplikaci).
- Schopnost zadání typu přestupku, údajů o přestupci a volba způsobu řešení.

- Úhrada pokut BKP
- Tisk dokladu o provedené revizi, nebo o úhradě pokuty.
- Úplná evidence provedených revizí a jejich výsledků. Minimálně je požadováno zobrazení sestavy obsahující následující položky:
 - Datum provedení revize
 - Revizor (identifikace pracovníka)
 - Linka a spoj
 - Číslo kontrolovaného nosiče a číslo jízdenkového produktu (jednotlivého nebo časového jízdního dokladu)
 - Výsledek kontroly
 - Záznam o kontrole

U sestavy je nutná možnost exportu do tabulek v požadovaném formátu: xls,xlsx a csv.

Základní požadované funkce aplikací Správa agendy revizorů a Správa mobilních zařízení

- Z PC je možno se přihlásit k **aplikaci pro správu agendy revizorů** s funkcemi:
 - správa a evidence revizorů (zavádění/evidence/vyřazení revizorů do/v/ze systému),
 - prohlížení výsledků kontrol revizorské činnosti (evidence stavu přestupku),
 - propojení na systémy zadavatele ekonomického a správního typu (evidence pokuty, podklady k úhradě pokuty na přepážce, podklady pro vymáhání pohledávek),
 - propojení na e-shop k řešení některých přestupků v systému.
 - zadavatel požaduje aplikaci ve formě webové aplikace.
- Z PC je možno se přihlásit k **aplikaci pro správu mobilních zařízení** s funkcemi:
 - správa připojených mobilních zařízení ve wi-fi (upgrade OS/SW bez nutnosti fyzického připojení zařízení kabelem),
 - správa dat (aktualizace dat v mobilních zařízeních)
 - zadavatel požaduje aplikaci ve formě webové aplikace.

Základní požadovaná funkce serverů:

V souladu s globálním požadavkem bude veškerá serverová část řešení aplikací správy agendy revizorů provozována v Technologickém centru Kraje Vysočina v prostředí serverové virtualizace (v duchu kap 3. Obecné požadavky).

Veškerá data jsou aplikačním serverem ukládána do databázového serveru nebo čtena z databázového serveru, na aplikačním serveru je pouze prezentační vrstva a aplikační logika.

Platební kanál banky bude zadavatel poptávat jako samostatnou službu a uchazeč jej nebude oceňovat do své nabídky.

Požadavky na mobilní zařízení pro revizory:

Součástí poptávky je dodávka 6-ti kusů mobilních zařízení pro revizory včetně příslušenství

Zařízení bude běžně používáno ve 3 modech, které si bude obsluha schopná přepínat při práci se zařízením (v kanceláři i v terénu):

1. Servisní mód:

Servisní funkce v kanceláři

- Před použitím provede revizor **aktualizaci SW a dat** (za využití bezdrátového připojení k síti, bez nutnosti fyzického připojení revizorského zařízení kabelem) v prostorách pracoviště, které je pokryto Wi-fi signálem. Použití Wi-fi umožňuje provést aktualizace v dostatečném objemu dat rychle a s minimálními náklady na přenosové služby.

Servisní funkce v terénu

- Při **aktualizaci** musí být zařízení schopno ze serveru stáhnout všechny potřebné údaje, tedy **BL, GL, WL** karet a kupónů (podle metody zvolené dodavatelem při řešení EOC VDV a také podle metod systémů ostatních akceptovaných identifikátorů), číselníky zón a profilů, seznam revizorů a konfigurační parametry a odeslána data o provedených kontrolách.
- V průběhu přepravní kontroly musí být možné kdykoliv provést **on-line dotaz** do centra nebo po přepnutí do základního režimu i provést **celou aktualizaci**.

2. Kontrolní mód

Kontrola v PAD (teoreticky využitelné i pro přepravní kontroly v železniční dopravě)

- Přiložením karty/ načtením QR kódu cestujícího na čtečku se provede kontrola

Kontrola v MHD

- Přiložením čtečky kontrolora k validátoru ve vozidle se Validátor přepne do revizorského módu. Přiloženému revizorskému zařízení předá validátor, taplist (v případě Chec in/check out).

- Přiložením karty načtením QR kódu cestujícího na čtečku revizora se provede kontrola

3. Platební mód

Platby bankovní kartou provedené revizorským zařízením jsou zasílány přímo do banky k realizaci (rozhraní banky pro platební terminály).

Komunikace a její zabezpečení:

SW Revizorského systému musí být schopen průběžně komunikovat s těmito okolními systémy:

- Skupinou mobilních zařízení (revizorských čteček)

Předpokládá se ověření (autorizace), vč. aktualizace, vyčtení počtu operací revizorského zařízení (kontrola výkonu revizora/kontrolora).

9 Popis whitelistů

Soubor strukturovaných dat whitelist bude využit pro poskytování informací o aktuálně platných kupónech, identifikaci držitele dopravního produktu (včetně zákaznické kategorie) a jeho kartách evidovaných v systému (jedinečných identifikátorech). Příjemcem a zpracovatelem whitelistu jsou dopravci, kteří na základě takto poskytnutých dat vyhodnocují nárok na přepravu a dále zajišťují proces přepravní kontroly cestujících. Systém umožní generovat whitelisty dle typu zapojeného subjektu (tj. rozsah poskytovaných dat bude určen na základě typu dopravce. Primárním cílem je zamezit distribuci osobních dat uživatelů pro subjekty/dopravce, kteří nebudou tyto údaje aktivně využívat pro svou činnost).

Whitelist musí obsahovat data aktuálně platných dopravních produktů a dle administrátorsky definované hodnoty bude možné ve whitelistu zachovat již neplatné produkty, nebo naopak produkty, u kterých ještě nenastala platnost (například: whitelist bude obsahovat produkty, jejichž platnost vypršela maximálně před 14 dny, nebo nastane za 2 dny).

Pokud budou z whitelistu odstraněny záznamy o všech zakoupených produktech zákazníka, tak automaticky budou odstraněny i osobní údaje zákazníka.

Pro personalizovaný typ bezkontaktní čipové karty dopravce by nemusela být ve whitelistu zanesena fotografie držitele karty (ztotožnění cestujícího by mohlo být realizováno vizuálně na základě předložení dopravní karty).

9.1 Základní definice struktury dat

Whitelist musí obsahovat minimálně níže uvedené údaje:

- Datové záznamy o cestujícím – uživateli systému (držiteli identifikátoru) minimálně v rozsahu:
 - Identifikátor držitele
 - Jméno
 - Příjmení
 - Datum narození
 - Fotografie držitele identifikátoru (v průkazovém formátu s optimalizované velikosti fotografie do maximální velikosti cca 2 kB)

-  Datové záznamy o zakoupeném dopravním produktu:
 - Identifikace tarifu
 - Identifikace zákaznické kategorie
 - Platnost tarifu od – do (včetně časové)
 - Definice územní platnosti (na základě výčtu povolených a vylitelných zón)
 - Definice vazby na identifikátor
- Datové záznamy o kartách (jedinečných identifikátorech)
 - ID jedinečného identifikátoru (tokenu)
 - Vlastní hodnota (datový záznam) jedinečného identifikátoru, ke kterému je dopravní produkt přiřazen
 - Typ jedinečného identifikátoru (bankovní karta, 2D čárový kód, karta dopravce)
 - Stav (platný/neplatný)
 - Vstupní hodnota pro vygenerování klíče určeného k dešifrování osobních údajů

Režim generování whitelistů

- Plný formát
 - Generování 1x denně
 - Obsahuje kompletní informace o produktech, identifikátorech a uživateli
 - Určen především do nového zařízení (popřípadě do zařízení, které nebylo delší dobu aktualizováno)
- Změnový formát (greenlist)
 - Obsahuje změny ve whitelistu oproti předchozímu stavu

Čas a četnost pravidelného generování whitelistu (green listu) bude možno spravovat administrátorem systému.

9.2 Zabezpečení osobních údajů

Osobní údaje o držiteli identifikátoru budou ve whitelistu zašifrovány (dle standardů šifrování, například: AES - Advanced Encryption Standard). Architektura přípravy whitelistu bude v nově budovaném systému implementována, tak aby každý záznam o uživateli systému byl zašifrovaný samostatně. Vstupní hodnota pro stanovení klíče bude odvozena až při vlastním použití daného identifikátoru zákazníkem, (požadavek na zajištění bezpečnosti dat z pohledu neoprávněného přístupu k osobním údajům.)

9.3 Číselníky tarifních dat

Vzhledem k datové úspoře při vlastní tvorbě (generování) whitelistů jsou jednotlivé informace o produktech (například zákaznická kategorie, označení tarifu apod.) interpretovány pouze identifikátorem, je tedy nutné vytvářet a distribuovat pro příjemce whitelistů převodní tabulky (číselníky).

Vlastní generování těchto číselníků musí zajišťovat Jádro systému elektronického odbavení cestujících a každý subjekt (příjemce whitelistu) musí v odbavovacím zařízení zabezpečit jejich příjem a zpracování.

Za správu a vydávání těchto číselníků bude odpovědný provozovatel systému, tj. subjekt určený VDV.

Rozhraní pro předávání dat (číselníků) mezi jádrem systému elektronického odbavení cestujících a subjektem (příjemcem whitelistu) bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například využitím webových služeb založených na principu REST, SOAP). Při návrhu rozhraní musí být kladen důraz na dodržení vysokých bezpečnostních standardů tohoto řešení.

10 Popis požadavků na zúčtovací centrum

Zúčtovací centrum musí zajistit evidenci všech transakcí (prodeje, storna, částečné užití produktu) vzniklých při prodeji dopravního produktu subjekty zapojenými do integrovaného dopravního systému VDV. Tento transakční přehled bude sloužit jako podklad pro výpočet podílu z tržeb pro jednotlivý subjekt zapojený do systému (dopravce).

Vzhledem k tomu, že hlavním identifikátorem cestujícího v systému EOC bude token, dodávaný zúčtovací systém bude spolupracovat s platební bránou (dodávka platební brány není součástí této poptávky), a to v předpokládaném cyklu zúčtování 1x 24 hodin.

Zadavatel předpokládá, že zúčtovací systém bude rozúčtovávat tržby z jízdného na základě předepsaného vzorce podílu tržeb na jednotlivé dopravce. Vlastní dělení tržeb bude realizováno modelem tzv. dohodnutého poměru (tj. maticí, která jasně určuje procentní podíl dopravce z celkového objemu tržeb za prodej dopravního produktu). Zadavatel požaduje, aby systém zúčtování evidoval všechny transakce provedené v systému EOC VDV a takto získaná data využil ke stínové kontrole zúčtování dle předepsaného vzorce. V rámci této funkce zadavatel požaduje provádět kontrolu transakčních dat (např. proti duplicitám).

Zúčtovací centrum musí minimálně umožnit:

- Definici a správu subjektů (dopravců) zapojených do systému
- Správu uživatelů a uživatelských rolí aplikace zúčtovacího centra
- Evidenci odbavovacích zařízení/prodejních míst za jednotlivý subjekt (dopravce)
- Evidenci mobilních zařízení revizora
- Příjem a zpracování transakcí za jednotlivá odbavovací zařízení (včetně rozlišení typu transakce: prodej, storno, částečné užití produktu)
- Příjem a zpracování dat (příp. transakcí) z mobilních zařízení revizora (např. zneplatnění jízdenky)

- Kontrolu vstupních a transakčních dat zaslaných do zúčtovacího centra z pohledu úplnosti (tj. identifikaci nedodaných transakcí a upozornění na takovou skutečnost)
- Realizaci výpočtu podílu dopravce z celkového objemu tržeb za prodej dopravního produktu
- Vytváření podrobných přehledů o zúčtování dat
- Zúčtování transakcí s různou hodnotou DPH
- Generování účetních podkladů (včetně vzájemných zápočtů mezi jednotlivými dopravci)
- Generování statistických podkladů
- Export všech výstupů do *.xls souborů

Požadovaný způsob návrhu aplikace zúčtovacího centra

Požadovaný způsob návrhu aplikace zúčtovacího centra je vytvoření webové aplikace, která bude přístupná ze sítě Internet na základě definovaného/povoleného rozsahu IP adres. Z pohledu bezpečnosti bude nutné využití zabezpečené komunikace se serverem prostřednictvím https protokolu. Přístupová oprávnění k aplikaci budou řešena na úrovni Administrátorské části systému.

Formát předávaných dat mezi subjektem integrované dopravy VDV (dopravcem) a zúčtovacím centrem bude realizován prostřednictvím XML zpráv.

Rozhraní pro komunikaci dopravce se zúčtovacím centrem bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například: využitím webových služeb založených na principu REST, SOAP). Při návrhu rozhraní musí být kladen důraz na dodržení vysokých bezpečnostních standardů tohoto řešení.

Dodavatel EOC VDV musí zajistit propojitelnost s vybavením dopravců VDV a s okolními zúčtovacími systémy další spolupracujících IDS krajů a měst. Jeho odpovědností bude navrhnout rozhraní a datovou větu pro komunikaci s těmito systémy.

11 Popis požadavků na datovou komunikaci (způsob distribuce dat)

11.1 Datové rozhraní pro distribuci whitelistů

Požadavky na datové rozhraní pro distribuci whitelistů

Rozhraní pro předávání dat uložených ve strukturovaném souboru whitelistu bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například: zabezpečený FTP server/SFTP, využitím webových služeb založených na principu REST, SOAP, ...). Je však nutné dodržet vysoké bezpečnostní standardy tohoto řešení.

Předávání dat (whitelistu) mezi systémem EOC a příjemcem whitelistu (dopravcem) bude realizováno prostřednictvím definovaného/navrženého rozhraní, které bude Zadavateli předáno v písemné formě při realizaci díla. Zadavatel se po předání díla stává vlastníkem uvedeného rozhraní a může jej bez dalšího omezení a licenčních poplatků používat i pro další účely.

11.2 Datová komunikace s externími systémy dopravců

Z důvodu požadavku na integraci nově budovaného systému EOC s kartově-odbavovacími systémy dalších dopravců, je nutné navrhnout a vybudovat rozhraní, které zajistí minimálně níže uvedené funkce:

Minimální požadavky na rozhraní pro datovou komunikaci s externími systémy dopravců

- Poskytnutí informací o uživateli systému (personalizační data)
- Ověření personalizačních dat uživatele systému
- Poskytnutí informací o registrovaných identifikátorech
- Předání dat o zákaznických kategoriích
- Potvrzení zákaznické kategorie uživatele (popřípadě vytvoření nové zákaznické kategorie)
- Nákup dopravního produktu dle postupů popsaných v kapitole 7.5
 - Výběr produktu dle tarifu
 - Výběr produktu pomocí kalkulátoru jízdného
 - Výběr pomocí vyhledávače spojení

- Storno dopravního produktu

Rozhraní pro komunikaci s externími systémy dopravců bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například: využitím webových služeb založených na principu REST, SOAP, ...). Zde je však opět kladen důraz na dodržení vysokých bezpečnostních standardů tohoto řešení.

Při realizaci prodeje/nákupu dopravního produktu (dle kapitoly 7.5) v kartově-odbavovacím systému dopravce je nutné vycházet z požadavku Zadavatele na jednotný způsob zpracování transakcí:

Požadavky na realizaci prodeje/nákupu dopravního produktu

- Vlastní proces nákupu musí být uskutečněn formou dotazování do systému EOC („tkzv. postupné sestavení produktu“). Na základě dotazu dopravce (kartově-odbavovacího systému) poskytne systém EOC soubor dat, který umožní další krok v sestavení produktu (například: dotazem na ověření cestujícího systém EOC poskytne údaje o uživateli a jeho zákaznických kategoriích; dalším krokem bude dotaz/požadavek na předání souboru tarifů ke zvolené zákaznické kategorii)
- Záznam o prodejní transakci (popřípadě stornu) bude vždy zaznamenán v systému EOC. Transakční data budou dále ze systému EOC předávána k zúčtování.
- Každý subjekt/dopravce, který bude komunikovat prostřednictvím toho rozhraní, musí být evidován v systému EOC (včetně jednotlivých prodejních míst).

Nově navržené rozhraní „Datová komunikace s externí systémy dopravců“ bude Zadavateli předáno v písemné formě v průběhu realizace díla. Zadavatel se po předání díla stává vlastníkem uvedeného rozhraní a může jej bez dalšího omezení a licenčních poplatků používat i pro další účely.

11.3 Datová komunikace s mobilními zařízeními revizorů

Pro možnost návrhu technických parametrů mobilních zařízení a odhadu objemu datové komunikace uvádíme následující předpoklady komunikace zařízení.

Ze zařízení budou odcházet tato data:

- Informace o zahájení kontrolní činnosti
- Informace o provedených kontrolách

- Chybové a stavové informace
- Komunikace na bankovní rozhraní platebních terminálů

Do zařízení budou přicházet tato data:

- Seznam zakázaných karet (BL)
- Seznam elektronických časových kuponů určený k nahrání (GL, vč. foto)
- Seznam přepravních kontrolorů
- Číselník názvů zón
- Číselník názvů profilů cestujícího
- Ostatní konfigurační parametry (pro technické nastavení zařízení)
- Informace o nahrání nových časových elektronických jízdenek

12 Bezpečnostní požadavky na systém

12.1 Základní požadavky na návrh systému

- Nově vybudovaný systém musí zajistit vysoký bezpečnostní standard tak, aby konkrétní data byla dostupná jen pro odpovědné osoby a subjekty. V tomto případě se nejedná pouze o zajištění bezpečnosti dat (zabezpečené uchovávání dat), ale zejména o proces jejich zpracování, které nesmí ohrožovat důvěrnost dat o uživateli systému.
- Bezpečnost musí být řešena nejenom z pohledu základní části systému elektronického odbavení cestujících, ale z pohledu bezpečnosti celého systému, tj. včetně dalších napojených systémů.
- Velký důraz je kladen na ochranu kryptografických klíčů použitých v systému tak, aby nemohlo dojít k jejich zpřístupnění (např. při odcizení odbavovacího zařízení, „nabourání“ do systému apod.).
- Dodavatel nesmí provádět žádné kroky vedoucí ke zjištění kryptografických klíčů použitých v systému (pokud nebude se Zadavatelem dohodnuto jinak).
- Systém musí být navržen tak, aby zajistil účinnou bezpečnost z pohledu důvěrnosti dat a nemožnosti zneužití (prolomení) systému např. formou využití cizích zařízení.
- Bezpečnost celého systému musí být řešena v souladu s platnou legislativou (zákonem o ochraně osobních údajů, platebním styku, dále musí být řešena v souladu s čl. 28 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů apod.).
- Řešení musí být navrženo tak, aby byla v maximální možné míře zajištěna bezpečnost dat (zajištění dat proti ztrátě, nekonzistenci, nežádoucí modifikaci a proti neoprávněnému přístupu).
- V celém Řešení se nebudou vyskytovat jakékoli nedokumentované funkcionality (tj. funkcionality SW, které nejsou popsány v žádné k tomu určené dokumentaci). Dodavatel zpracuje bezpečnostně-provozní dokumentaci ve fázi zpracování Prováděcího projektu. Součástí této dokumentace bude mimo jiné i bezpečnostní specifikace, tedy popis všech funkcí prosazujících zajištění dostupnosti, důvěrnosti a integrity zpracovávaných dat. Rozsah, strukturu a obsah bezpečnostně-provozní dokumentace určí zadavatel ve fázi zpracování Prováděcího projektu, přičemž tyto požadavky budou pro Dodavatele závazné a nesmí se promítnout v navýšení celkové nabídkové ceny.

- V celém Řešení budou všechny operace a činnosti provedené uživateli a administrátory zaznamenávány formou logů a auditních záznamů. Formát, obsah, rozsah, strukturu a úroveň logování a auditování určí zadavatel ve fázi zpracování Prováděcího projektu, přičemž tyto požadavky budou pro Dodavatele závazné a nesmí se promítnout v navýšení celkové nabídkové ceny.
- Dodavatel ve fázi zpracování Prováděcího projektu navrhne způsob provozního a bezpečnostního monitoringu celého řešení a ve fázi implementace jej po schválení zadavatelem nasadí.
- Dodavatel provede podrobnou a komplexní analýzu rizik informační bezpečnosti v souvislosti jak s nasazením Řešení, tak i s provozem tohoto Řešení. Analýza rizik informační bezpečnosti musí být zpracována před nasazením do provozního režimu. Dodavatel vypracuje a předá zadavateli:
 - zdokumentovaný postup provedení analýzy rizik (metodiku, jak postupoval),
 - zprávu z analýzy rizik obsahující vydefinovaná a klasifikovaná rizika, která jsou určena na základě míry dopadu, pravděpodobnosti výskytu zranitelnosti a pravděpodobnosti naplnění hrozby, a popis těchto rizik,
 - plán zvládnutí rizik s návrhy opatření na snížení míry případných rizik včetně popisu způsobu jejich nasazení.
- Řešení může být podrobeno důkladnému penetračnímu testu ve fázi jeho testování. Dodavatel zajistí řešení případných bezpečnostních chyb, nedostatků či zranitelností, pokud budou testem objeveny. Službu penetračních testů zajišťuje zadavatel, Řešení nebude převzato do provozního režimu do doby vyřešení případných bezpečnostních zranitelností.
- Úrovně všech přístupových oprávnění/jednotlivých rolí musí být detailně popsány v provozně bezpečnostní dokumentaci řešení.
- Aplikační servery, moduly či jiné části řešení (např. web server, DB server, apod.) nesmí vyžadovat pro své spuštění privilegovaná oprávnění (např. typu root, Administrator, NT Authority\System, apod.)
- Každý uživatel řešení musí být unikátní (musí mít jednoznačný identifikátor) a personifikovaný s výjimkou systémových účtů, které musí naplňovat jmennou konvenci, kterou stanoví zadavatel a pro Dodavatele je tato konvence závazná.

- V řešení nesmí existovat sdílený uživatel pro více fyzických uživatelů. Pokud je sdílený uživatel nezbytný, musí se buď jednat o systémový účet neumožňující interaktivní přihlášení, nebo použití takového účtu musí být řádně logováno – musí existovat auditní stopa o tom, kdo a v jaký čas roli sdíleného uživatele převzal.
- V případě potřeby použití účtů typu "super administrátor" (privilegovaný uživatel s možností převzít na sebe roli někoho jiného) je nutné dodržovat tato pravidla:
 - použití jiného uživatele prostřednictvím "superadministrátora" musí být zaznamenáno v auditní stopě,
 - všechny operace provedené „superadministrátorem“ musí být logovány,
 - superadministrátor musí být v IS zaveden formou role (nikoliv 1 uživatelského účtu).
- Zrušení uživatele musí vždy probíhat formou jeho zneplatnění či zneaktivnění, nikoliv jeho vymazáním z důvodu zachování auditní stopy.

12.2 Speciální požadavky na návrh systému

Zvýšené požadavky na systém uvedené v této kapitole se týkají pouze následujících funkcionalit systému EOC:

- ✓ Registrace cestujících (přiřazení jednoznačného identifikátoru k účtu vnějšího uživatele)
 - ✓ Volitelná registrace a autentizace cestujících prostřednictvím elektronické identity (NIA)
 - ✓ Založení a správa uživatelského účtu zákazníka (cestujících)
 - ✓ Uchování osobních dat uživatelů systému (archiv osobních údajů cestujících)
 - ✓ Správa životního cyklu uživatelů systému EOC VDV (vnějších i vnitřních)
 - ✓ Správa zákaznických profilů/kategorií u cestujících
 - ✓ Realizace změnových požadavků při správě osobních údajů cestujících
 - ✓ Správu identifikátorů
 - ✓ Správa zakoupených produktů
 - ✓ Správa cizích subjektů a dopravců jako uživatelů systému
 - ✓ Založení uživatelských účtů vnitřních uživatelů systému (ne cestujících)
 - ✓ Ověření vnitřních uživatelů systému (prostřednictvím SSO KV a IDM KV)
 - ✓ Správu uživatelů a uživatelských rolí vnitřních uživatelů systému
 - ✓ Komunikace se servery provozovanými v Technologickém Centru Kraje Vysočina
 - ✓ Komunikace s externími systémy při procesu ověřování identifikátorů EOC VDV
- Řešení musí podporovat tyto formy vícefaktorové autentizace běžných uživatelů a správců/administrátorů díla, přičemž uživatel si bude volit způsob silného ověřování:

- U2F/FIDO2
- OTP generovaný mobilní aplikací
- OTP zasílaný přes SMS

V rámci zpracování prováděcího projektu bude dojednáán rozsah použití nástroje pro autentizaci uživatelů při konkrétních funkcích EOC, přičemž zadavatelem určené metody autentizace budou pro dodavatele závazné a nesmí se promítnout v navýšení celkové nabídkové ceny.

Požadavky na vícefaktorovou autentizaci se netýkají systémových účtů.

- Veškeré kryptografické funkce a algoritmy musí být v souladu s interními standardy zadavatele.
- Řešení musí umožňovat granulační řízení přístupových oprávnění k osobním údajům, tzn., musí existovat možnost přidělení oprávnění konkrétní roli/uživateli ke konkrétním typům/sadám osobních údajů pro konkrétní typ operace (čtení, zápis, mazání,...).

12.3 Základní požadavky na zabezpečení komunikace

- Jednotlivé části systému mezi sebou komunikují s využitím dostupných technologií – internet, TCP/IP. Veškerá komunikace probíhá s využitím kryptografie a šifrování minimálně na aplikační vrstvě, případně i na transportní vrstvě. V případě přenosu GSM/GPRS, 3G, LTE jsou SIM karty speciálně zabezpečeny (APN, VPN). Při návrhu celého systému je nutné dodržet vysoké bezpečnostní standardy pro datovou komunikaci.

12.4 Speciální požadavky na zabezpečení komunikace

Zvýšené požadavky na zabezpečení komunikace uvedené v této kapitole se týkají pouze funkcionalit systému EOC uvedených v kapitole 12.2

• HTTP Headers

Všechny webové servery musí být nakonfigurovány tak, aby zajišťovaly maximální možnou míru bezpečnosti informací a pro webové uživatelské rozhraní naplňovaly minimálně následující požadavky na bezpečnostní http hlavičky:

- X-Frame-Options
 - Musí být implementována (tzn. server ji musí klientské aplikaci zasílat)
 - Záhloví může nabývat pouze hodnot DENY nebo SAMEORIGIN dle potřeby
- Strict-Transport-Security
 - Musí být implementována
 - Direktiva max-age musí nabývat hodnoty minimálně 31536000
 - Ostatní direktivy jsou volitelné
- Content-Security-Policy
 - Musí být implementována
 - Aktiva mohou být načítána pouze prostřednictvím zabezpečeného protokolu (direktiva https:)
 - Aktiva mohou být načítána pouze z konkrétních a bezpečných zdrojů
 - Pokud by bylo nutné načítat aktiva z jiných zdrojů, které nejsou umístěny na infrastruktuře, která je v držení zadavatele nebo dodavatele, podléhají tyto zdroje nejprve schválení zadavatelem. Pokud ke schválení zadavatelem nedojde, tyto zdroje nemohou být použity k načítání aktiv spolu se zbytkem webové stránky
- X-Content-Type-Options
 - Musí být implementována
- Referrer-Policy
 - Musí být implementována
 - Nesmí obsahovat direktivy: prázdný string, unsafe-url
- Permissions-Policy
 - Musí být implementována
 - Mohou být povolena pouze ta oprávnění, která jsou skutečně a aktuálně potřeba, všechna ostatní musí být explicitně zakázána
- X-XSS-Protection
 - Musí být implementována
 - Direktiva politiky musí nabývat hodnoty 1; mode=block
- Server
 - Pokud je hlavička implementována, musí být změněna tak, aby neodhalovala citlivé informace odhalující verzi webového serveru

- Set-Cookie
 - o Pokud se jedná o session cookies, musí obsahovat direktivu nastavující secure a httponly flagy.
- Cross-Origin-Embedder-Policy
 - o Musí být implementována
- Expect-CT
 - o Musí být implementována
- Cross-Origin-Opener-Policy
 - o Musí být implementována
- Cross-Origin-Resource-Policy
 - o Musí být implementována

13 Požadavky na mobilní aplikaci systému elektronického odbavení cestujících

Součástí celého řešení bude i dodávka mobilní aplikace, která zajistí shodné funkce odbavení uživatele systému EOC popsané v kapitole 5 „Požadavky na samoobslužný systém pro odbavení zákazníků (portál zákazníka, e-shop)“.

Aplikace musí být navržena minimálně pro provozování na mobilních zařízeních s operačním systémem Android (od verze 5.0 a dále) a iOS (od verze 11.0 a dále). Dále musí splňovat požadavek na veřejnou dostupnost v obchodech Apple Store (App Store), Google Play (Obchod Play).

Mobilní aplikace samoobslužného systému pro odbavení cestujících musí mít tyto základní funkce:

- Zobrazení profilu zákazníka v mobilní aplikaci (včetně fotografie), zobrazení zakoupeného produktu a identifikátoru (QR kódu)
- Založení a správa uživatelského účtu zákazníka (při personalizaci účtu bude pořízená fotografie uživatele – realizováno prostřednictvím integrovaného fotoaparátu mobilního zařízení, nebo načtením souboru z paměti tohoto zařízení)
- Funkce pro přiřazení identifikátorů k účtu uživatele
- Správa těchto identifikátorů
- Správa zakoupených produktů
- Správa zákaznických profilů/kategorií
- Nákup a úhrada dopravního produktu
- Nákup a úhrada jednorázových časových jízdenek

Zadavatel požaduje otevřenost mobilní aplikace k budoucímu propojení s datovým rozhraním aplikace pro veřejnost Centrálního dispečinku VDV, a to za účelem vyhledání spojení a jeho zobrazení na mapovém podkladu.

Poznámka:

Řešení musí vycházet z dostupných metod vývoje mobilních aplikací pro operační systémy Android a iOS. Z důvodu zjednodušení správy/udržování mobilní aplikace je požadováno využít k jednotlivým výše uvedeným funkcím aplikace tzv. zobrazení responzivních webových stránek systému „portál zákazníka,

e-shop“ (jak je popsáno v kapitole 5.) Jiný přístup vyžadujeme u funkcí: generování identifikátoru, zobrazení zakoupeného dopravního produktu a nákup jednorázových jízdenek kde nelze využít responzivních webových stránek systému „portál zákazníka, e-shop.

Minimální požadavky na jedinečný identifikátor mobilní aplikace

- Identifikátor bude unikátní pro každou jednotlivou instalaci mobilní aplikace v telefonu i v rámci jednoho uživatelského účtu (z uvedeného vychází i požadavek na unikátnost v rámci instalace do různých mobilních zařízení)
- Identifikátor bude automaticky přiřazen k účtu uživatele (pro možnost nákupu a přiřazení dopravního produktu)
- Systém EOC musí zajistit rozlišení tohoto typu identifikátoru

Mobilní aplikace musí zajistit vytvoření/vygenerování jedinečného identifikátoru mobilní aplikace, který bude prezentován formou QR kódu na displeji mobilního zařízení, aby na jeho základě mohl být vypočítán token a vyhledán příslušný záznam ve whitelistu. Token mobilní aplikace bude počítat dedikovaný proces v Back office EOC (respektive SAM při off-line tokenizaci ve vozidle) stejně jako u ostatních identifikátorů typu QR kód a BČK. Tokenizační algoritmus zůstává stejný jako u ostatních identifikátorů typu QR kód a BČK.

Generovaný QR kód musí být zabezpečen možností ověření získaných dat.

Mobilní aplikace, která bude tento QR kód zobrazovat musí zajistit ochranu proti vytvoření tzv. snímku obrazovky (například: využití dynamického QR kódu apod.).

Minimální požadavky na definici jednorázových časových jízdenek:

Pro funkci „Nákup a úhrada jednorázových časových jízdenek“ musí být systém EOC vybaven modulem pro správu těchto produktů. Ke každému subjektu, zavedenému v systému EOC bude umožněno samostatně definovat soubor těchto produktů.

- Unikátní identifikátor jízdenky/tarifu
- Označení jízdenky (slovní popis)
- Definice územní platnosti

- Definice časové platnosti
- Omezení platnosti jízdenky (například na den v týdnu)
- Omezení zahájení platnosti (čas nutný pro zahájení platnosti jízdenky po jejím nákupu a vygenerování)
- Kategorie zákazníka
- Cena

Z důvodu požadavku na okamžité ověření platnosti jednorázové jízdenky je nutné výše uvedená data doplnit do generovaného QR kódu, tj. umožnit realizaci ověření platnosti jízdenky prostřednictvím načtení QR kódu. Ochrana těchto dat proti zneužití musí vycházet z výše uvedených požadavků.

14 Součinnost zadavatele

Níže specifikované systémy, komponenty systémů, strategické dokumenty a služby nejsou součástí poptávky a jejich specifikace slouží k informování uchazeče o návaznostech na stávající vybavení zadavatele a jeho spolupracujících subjektů v projektu.

14.1 Odbavovací zařízení dopravců (strojky dopravců)

Tato kapitola popisuje základní požadavky na odbavovací zařízení dopravců zapojených do integrovaného dopravního systému VDV (jedná se o specifikaci požadavků, které jsou předávány stávajícím, nebo nově soutěženým dopravcům).

Odbavovací zařízení dopravců provádí akceptaci (odbavení) dopravního produktu zakoupeného prostřednictvím systému elektronického odbavení cestujících.

Pro zajištění výše uvedené funkce musí být odbavovací zařízení minimálně vybaveno:

(požadavky na vybavení odbavovacího zařízení, které zadavatel předal dopravcům, jako přílohu k nové smlouvě na dopravní obslužnost)

- Čtečkou bezkontaktních čipových karet dle ISO 14443 A/B (Mifare Standard, Mifare DESfire EV1). Tato čtečka bude dále vybavena minimálně 4 sloty pro SAM paměťové kontaktní karty dle ISO 7816.
- Platebním terminálem (akceptačním zařízením bankovních karet) s certifikovaným EMV level 1 a 2 kernelem se schopností akceptovat bezkontaktní karty modelů VISA a Mastercard

- Zadavatel požaduje, aby odbavovací zařízení bylo vybaveno čtečkou NFC pro případné budoucí využití při akceptaci mobilního telefonu jako identifikátoru nebo platebního nástroje prostřednictvím rozhraní NFC.

(výše uvedená tři zařízení mohou být sloučena do jednoho HW modulu)

- Pro úlohu generování jednoznačného identifikátoru je nutné zařízení vybudovat tak, aby splňovalo požadavky PCI DSS (například řešení vybudované v souladu se standardem PTP /Point-to-Point Encryption/). Některá odbavovací zařízení staršího typu požadavky PCI DSS nemusí splňovat.
- *Optickou čtečkou 2D čárového kódu*, která musí splňovat minimálně níže uvedené parametry:
 - Zpracování 2D kódu typu: QR kód
 - Korekce: Level L (8%)
 - Verze: 23 (109 x 109 modulů)
 - Zpracování (načtení) QR kódu musí být realizováno cca do 1500 ms (v případě dynamicky zobrazovaného QR kódu bude jeho další část zpracována do 1100 ms)

- *LCD panelem minimální velikosti 9" s rozlišení minimálně 800x600 bodů a hloubkou barev 32-bitů.* Tento panel musí být uzpůsoben tak, aby zajišťoval dobrou viditelnost na přímém slunci. Dále musí splňovat požadavky na vyšší odolnost zařízení (z pohledu každodenního použití minimálně 10 hodin, provozní rozsah teplot od -20°C od 50°C, apod.)

LCD panel bude mj. zajišťovat zobrazení informací o dopravním produktu a držiteli karty (včetně fotografie průkazového formátu) získaných z whitelistu

- *Interní paměť*, která zajistí uložení a zpracování souboru strukturovaných dat whitelistu, o minimální velikosti 1 GB
- *Modulem pro zajištění mobilní datové komunikace* standardu GPRS, 3G, LTE (určené minimálně pro aktualizaci whitelistu).
- *Výpočetní jednotkou (řídícím PC)* jehož výpočetní výkon zajistí zpracování dat whitelistu do maximálně 500 ms. Některá odbavovací zařízení staršího typu tyto požadavky nemusí splňovat.

Zpracováním dat z Whitelistu se rozumí:

vyhledání záznamu dle načteného jedinečného identifikátoru, dešifrování osobních dat držitele identifikátoru a jejich zobrazení, vyhodnocení platnosti dopravního produktu a jeho zobrazení).

Odbavovací zařízení dopravce musí dále zajistit:

- Realizaci funkcí symetrické a asymetrické kryptografie (dešifrování osobních dat držitele karty, ověření jedinečnosti QR kódu)
- Pravidelnou komunikaci s rozhraním pro předávání dat strukturovaných souborů whitelistu a číselníků (odbavovací zařízení musí zajistit podporu standardně používaných technologií pro výměnu dat mezi systémy (například: zabezpečený FTP server/SFTP, využití webových služeb založených na principu REST, SOAP). Četnost této komunikace (pravidelný interval) bude možné libovolně upravovat. (zadavatel předpokládá z hlediska praktického využití, že interval zasílání nebude delší než 15 minut)
- Generování transakčních dat o prodeji/(akceptaci-použití) dopravního produktu a jejich přenos do zúčtovacího systému.

Základní popis procesu odbavení:

- Načtení vstupních dat pro výpočet jedinečného identifikátoru (tokenu) z uživatelem předloženého média (bankovní karta, dopravní karta, QR kód mobilní aplikace)
- Vygenerování jedinečného identifikátoru
- Vyhledání jedinečného identifikátoru ve whitelistu
- Získání příslušných dat z whitelistu (osobní data uživatele, zakoupený dopravní produkt)
- Vyhodnocení územní a časové platnosti zakoupeného dopravního produktu v aplikačním software odbavovacího zařízení. (dle aktuálně zvolené trasy/linky)
- Případný výpočet/dopočet ceny jízdného dle zvolené trasy/linky
- Zobrazení výsledku vyhodnocení územní a časové platnosti dopravního produktu (včetně informace o případném doplatku), zobrazení osobních dat uživatele (včetně fotografie a zákaznické kategorie)
- Realizace možného doplatku za jízdné

Další požadavky na odbavovací zařízení

Pro případ aktuálního, nebo budoucího vybavení odbavovacího zařízení validátorem (typicky při sdílení vozidla v systému PAD a MHD), musí zařízení disponovat funkcí módu revize, kdy po přiložení čtečky kontrolora k validátoru se validátory zablokují pro prodej JD.

Další požadavky na odbavovací zařízení mohou být zadavatelem specifikovány v průběhu realizace projektu.

14.2 MAP SAM moduly

Zadavatel disponuje uvedenými SAM moduly v počtu 400ks s možností navýšení jejich počtu.

MAP SAM modul v systému EOC VDV slouží k:

- Výpočtu tokenu pro identifikátory typu QR kód a BČK
- Ověření pravosti In Karty Českých drah

Specifikace SAMů ODP

Terminálový SAM ve verzi alespoň 1.0.85, který obsahuje

- tokenizační klíč EOC VDV
- veřejný klíč pro ověření pravosti In Karty
- čtecí klíč In Karty
- tokenizační algoritmus pro identifikátory typu QR kód a BČK

Funkce SAM

- *Autentizace odbavovacího zařízení k SAM modulu* – pomocí autentizačního klíče, uloženého v paměti odbavovacího zařízení. (Autentizační klíč k ostrým SAMům bude dodavatelům odbavovacích zařízení předán bezpečnou cestou v průběhu projektu.)
- *Výpočet tokenu* – token je v SAMu počítán ze vstupních dat za pomoci tajného kryptografického klíče.
- *Ověření platnosti In Karty* – před další prací s In Kartou musí odbavovací zařízení ověřit, zda se jedná o pravou kartu. Odbavovací zařízení proto pomocí SAMu ověří, že In Karta disponuje správnými kryptografickými klíči.

- Aktualizace SAM – v současné době může proběhnout pouze manuálně-off-line (mimo odbavovací zařízení).

14.3 Tokenizační mechanismus

*Tokenizací se rozumí kryptografická operace, která bezpečně převádí hodnotu zvoleného identifikátoru na hodnotu zástupnou, tzv. token. Samotný postup, pomocí kterého je z hodnoty identifikátoru, za pomoci tajného klíče, token získán, nazýváme *tokenizačním algoritmem*.*

Principy bezpečnosti

- *Tokenizační algoritmus je důvěrný* a smí být poskytnut pouze těm subjektům, které ho přímo implementují ve svých zařízeních, tedy poskytovatel, platebních terminálů nebo dodavatelům SAM modulů Kraje Vysočina, případně partnerských SAM modulů.
- *Tokenizační klíč v držení Kraje Vysočina je tajný* a může být předáván pouze bezpečnou cestou za dodržení všech podmínek bezpečnostní politiky Kraje Vysočina (ideálně tedy přímo v bezpečném HW úložišti – HSM, SAM modulu..., případně zašifrovaný transportním klíčem a rozdělený pro přenos do několika nezávislých komponent).

Poznámka

Zadavatel je v současné době vybaven tokenizačním klíčem a tokenizačním algoritmem. Zadavatel požaduje využití tohoto klíče i algoritmu při tokenizaci identifikátorů typu QR kód a BČK v systému EOC VDV.

U Bankovní karty jedinečný identifikátor – Token bude počítat pouze platební brána, **proces tokenizace BPK tedy není součástí poptávaného systému.**

Alternativa k tokenizaci identifikátorů typu QR kód a BČK

Zadavatel nevylučuje použití alternativního způsobu identifikace cestujícího v systému EOC a to pouze použitím vstupních dat (číslo karty, expirace, číslo QR kódu).

Vše za předpokladu dodržení všech bezpečnostních standardů.

Podrobnější popis tokenizačního mechanismu je uveden v příloze č.2

14.4 Platební brána

Platební brána bude soutěžena v samostatném výběrovém řízení. Popis rozhraní platební brány bude Zhotoviteli předán nejpozději v průběhu přípravy prováděcího projektu.

Platební brána bude pracovat v souladu se standardy PCI DSS a její dodavatel bude motivován k dosažení propojitelnosti a zprovoznění plné funkčnosti vazeb mezi systémy EOC a Platební brány.

14.5 Materiály a dokumentace pro nastavení systému zúčtování

Zadavatel pro přípravu zúčtovacího systému předloží při podpisu smlouvy dodavateli tyto strategické dokumenty v aktuálním znění:

- Tarif (Stávající znění je k dispozici na webu zadavatele)
- Převážně smluvní podmínky (Stávající znění je k dispozici na webu zadavatele)
- Algoritmy pro rozúčtování tržeb při přejezdech spojů přes hranice IDS. Zadavatel předpokládá budoucí vzájemné uznávání jízdních dokladů s okolními IDS.
- Zadání pro dělení tržeb (Koeficienty, matice, vzorce a další)

Zadavatel předpokládá, že zúčtovací systém bude rozúčtovávat tržby z jízdného na základě předepsaného vzorce podílu tržeb na jednotlivé dopravce. Vlastní dělení tržeb bude realizováno modelem tzv. dohodnutého poměru (tj. maticí, která jasně určuje procentní podíl dopravce z celkového objemu tržeb za prodej dopravního produktu).

14.6 Analýza k tvorbě QR kódu dle datové struktury MAP

Zadavatel disponuje analýzou a návrhem struktury QR kódu včetně podrobného popisu doporučené datové struktury MAP.

Datová věta, složená dle datové struktury MAP a uložená do QR kódu, je definována jako struktura REC_MAPPHONE_DATA v dokumentu MAP Karta – Datové struktury (verze 13), kterou mají k dispozici dodavatelé prodejních a odbavovacích zařízení.

Zadavatel požaduje využití tohoto návrhu v procesu generování QR kódu mobilní aplikací. QR kód slouží (vedle BČK dopravců a BPK) jako jedinečný identifikátor v systému EOC. QR kód bude generován mobilní aplikací a zobrazen na displeji elektronického zařízení.

Podrobný popis návrhu datové věty bude předán zhotoviteli nejpozději v průběhu přípravy Cílového konceptu

14.7 ISIC

Zadavatel požaduje spolupráci systému EOC s API rozhraním do DB ISICu pro on-line ověřování studentských průkazů.

Je k dispozici API rozhraní do DB ISICu pro on-line ověřování studentských průkazů. Dotaz do API je zdarma. Pro odladění služby je k dispozici testovací DB dostupná na webu vydavatele ISIC.

14.8 Využití přístupového bodu NIA

Zadavatel požaduje nastavit přihlašovací a registrační systém EOC tak, aby umožňoval volitelně také využití přístupového bodu NIA (Národního bodu pro autentizaci a identifikaci) při procesu registrace a přihlášení uživatele do systému EOC.

Příloha č. 1 – Základní popis předpokládané implementace EOC ve VDV

Základní popis (definice) stávajícího Integrovaného dopravního (tarifního) systému Veřejné dopravy Vysočiny je obsažen v dokumentech Smluvních přepravních podmínek a dalších na webu:

<https://www.kr-vysocina.cz/tarif%2Dvdv/ds-304441/p1=106091>

Při implementaci nového systému EOC se předpokládá, že jízdní doklady budou ukládány na nosičích a identifikátorech:

Název	Způsob úhrady	Nosič (identifikátor)
obyčejná jednosměrná jízdenka	hotovost, BČK dopravce, BPK	papír, mobilní aplikace - QR kód, BČK dopravců, BPK
celodenní jízdenka-síťová jízdenka	hotovost, BČK dopravce, BPK,	papír, mobilní aplikace - QR kód, BČK dopravců, BPK
roční síťová jízdenka	hotovost, BPK	mobilní aplikace - QR kód, BČK dopravců, BPK
jednozónová jízdenka (i v případě integrace MHD)	hotovost, BČK dopravce, BPK	papír, mobilní aplikace - QR kód, BČK dopravců, BPK
integrovaná sedmidenní jízdenka	hotovost, BPK,	mobilní aplikace - QR kód, BČK dopravců, BPK
integrovaná třicetidenní jízdenka	hotovost, BPK,	mobilní aplikace - QR kód, BČK dopravců, BPK
integrovaná devadesátidenní jízdenka	hotovost, BPK	mobilní aplikace - QR kód, BČK dopravců, BPK
předplatné MHD (v případě integrace MHD)	hotovost, BPK	mobilní aplikace - QR kód, BČK dopravců, BPK, karta dopravce dané MHD (např. Jihlavská karta)

Prodej roční síťové jízdenky a předplatného pouze na předprodeji (prodejní místo dopravce, portál zákazníka-e-shop, mobilní aplikace)

Jako u stávajícího tarifu, za platný jízdní doklad ve vyjmenovaných linkách VDV a jejich vyznačených úsecích dle přílohy č. 2 SPP VDV bude uznáván i jízdní doklad IDS JMK, IREDO, SID a PID včetně dokládání nároku na slevu.

Poznámka

U BČK dopravců předpokládáme pouze technologii karet Mifare DesFire, Mifare Desfire EV1. Karty Mifare Classic (Standard) využívané v současnosti u dopravců nebudou v systému akceptovány. BČK dopravců bude v systému EOC využívána jako identifikátor pouze pro tokenizované transakce – viz příloha č. 2

Příloha č. 2 – Požadavky na vytvoření tokenu z údajů získaných z identifikátorů systému EOC

Každý identifikátor se v systému eviduje pod speciálním jedinečným číslem (tzv. tokenem). Tento token se používá, aby se v systému neuchovávaly potenciálně zneužitelné údaje (například číslo bankovní karty). Token je potřeba spočítat vždy, když se do systému přidává nový identifikátor nebo když se mají v systému vyhledat informace svázané s konkrétním identifikátorem.

Tokenizace BPK

Identifikátor typu BPK (bezkontaktní platební karta) bude tokenizován dodavatelem platební brány a tato tokenizace není součástí poptávaného systému EOC. Platební brána bude pracovat v souladu se standardy PCI DSS a bude používat vlastní tokenizační algoritmus a klíč.

Tokenizace identifikátorů typu QR kód a BČK

Výpočet tokenu z identifikátoru provádí speciální služba, která alternativně může být součástí poptávaného systému EOC (prvotní on-line tokenizace při registraci) nebo SAM modul v odbavovacím zařízení (off-line tokenizace). Tokenizační algoritmus a klíč používaný službou EOC a odbavovacího zařízení je totožný. Tento algoritmus a klíč je platný pouze pro tokenizaci identifikátorů typu QR kód a BČK v EOC

Alternativa k tokenizaci identifikátorů typu QR kód a BČK

Zadavatel nevylučuje použití alternativního způsobu identifikace cestujícího v systému EOC, a to pouze použitím vstupních dat (číslo karty, expirace, číslo QR kódu) původně určených k tokenizaci. Vše za předpokladu dodržení všech bezpečnostních standardů.

Výpočet tokenu při registraci nového identifikátoru v systému

Při prvotní on-line registraci identifikátorů typu QR kód a BČK token generuje služba EOC. Vypočtený token zasílá do Backoffice VDV.

- Uživatel, který se bude registrovat pomocí BČK dopravce (např. IN-karty, Jihlavské karty), bude do systému zaregistrován pouze na základě zadání čísla karty, případně její expirace
- Uživateli, který se do systému bude registrovat pomocí QR kódu, bude přiřazen QR kód vygenerovaný za pomoci mobilní aplikace
- Uživatel, který se bude registrovat pomocí bankovní karty (BPK), bude během registrace do systému přesměrován na platební bránu, která provede ověření karty a výpočet tokenu. Token zašle do Back office EOC. Vše je řešeno v integrovaném prostředí front-endu EOC (např. e-shop) a platební brány

Výpočet tokenu v odbavovacím zařízení dopravce při použití BPK

Při odbavení ve vozidle/vlaku/na přepážce bude výpočet tokenu realizován v odbavovacím zařízení dopravce za pomoci akceptačního zařízení bankovních karet/platebního terminálu s certifikovaným EMV level 1 a 2 kernelem se schopností akceptovat bezkontaktní karty modelů VISA a Mastercard.

Čtečka bankovních karet bude zajišťovat jak funkci generování jedinečného identifikátoru bankovní karty, tak platební funkci (tj. umožní úhradu jízdného prostřednictvím bankovní karty). Pro úlohu generování jednoznačného identifikátoru, akceptační zařízení bankovních karet musí splňovat požadavky PCI DSS (například řešení vybudované v souladu se standardem PTPE /Point-to-Point Encryption/).

Proces tokenizace ve vozidle bude plně v režii dodavatele platební brány.

Výpočet tokenu v odbavovacím zařízení dopravce při použití identifikátorů typu QR kód a BČK

Při odbavení ve vozidle/vlaku/na přepážce bude výpočet tokenu realizován v odbavovacím zařízení dopravce za pomoci SAM modulu.

Algoritmus pro výpočet jedinečného identifikátoru (tokenu) BPK:

Tokenizační algoritmus a klíč bude jedinečný a jeho implementace do SW prostředí odbavovacího zařízení bude plně v režii dodavatele platební brány.

Algoritmus pro výpočet jedinečného identifikátoru (tokenu) identifikátorů typu QR kód a BČK

Tokenizační algoritmus a klíč bude jedinečný. V odbavovacím zařízení bude tokenizační algoritmus bezpečně uložen přímo v SAM modulu, který provádí vlastní výpočet tokenu.

Příklady výpočtu vstupních dat pro tokenizační algoritmus

Vstupní data budou dosazena do tokenizačního algoritmu (vzorce)

U bankovní karty (BPK) pro výpočet vstupních dat budou použity následující údaje vytištěné na těle nosiče:

- Číslo karty
- Expirace

U In Karty (na platformě MAP s nosičem Mifare DESFireEV1) pro výpočet vstupních dat budou použity následující údaje vytištěné na těle nosiče:

- Číslo karty (PAN)
- Expirace karty

U Jihlavské karty (na nosiči Mifare DESFire) bude pro výpočet vstupních dat využito:

- UID karty Mifare DESFire dle standardu ISO-14443A (resp. číslo Jihlavské karty)

Hodnota UID není z karty lidským okem čitelná (na rozdíl od čísla Jihlavské karty). Pro případnou registraci Jihlavské karty prostřednictvím webového rozhraní bude nutné vytvořit v Backoffice EOC KV převodní službu, která zajistí převod čísla Jihlavské karty na UID a zároveň dotazem do Backoffice DPMJ ověří platnost Jihlavské karty.

U mobilní aplikace (QR kódu) bude pro výpočet vstupních dat použit jednoznačný identifikátor kódovaný do pole bajtů a předávaný v QR kódu v části „Datová část specifická pro zákazníka“. Vnitřní strukturu tohoto identifikátoru tento dokument nepopisuje; bude stanovena dodavatelem mobilní aplikace.

Poznámka

Systém musí být navržen tak, aby umožňoval budoucí zapojení dalších dopravců, u kterých mohou být použity odbavovací technologie využívající BPK, nebo karet Mifare DesFire, Mifare Desfire EV1.

Karty Mifare Classic (Standard) využívané v současnosti u dopravců nebudou v systému akceptovány

Příloha č. 2
Smlouvy o dílo

Podmínky akceptace

Předání a převzetí Díla a jeho částí proběhne v souladu s podmínkami uvedenými níže:

Dílo se skládá z následujících logických celků:

1. Prováděcí projekt (zpracovaný na základě TZD)
2. Back office EOC
 - Jádro systému
 - Správa systému
 - Správa osobních dat
3. Samoobslužný systém pro odbavení zákazníků
4. Systém administrace
5. Prodejní portál
6. Systém mobilních zařízení pro revizory
7. Zúčtovací systém
8. Mobilní aplikace systému EOC
9. Komunikační rozhraní systému

Základní požadavky a rámce pro akceptační postup při předávání Díla a jeho částí Objednateli

Níže jsou uvedené základní požadavky a rámce pro akceptační postup při předávání Díla a jeho částí Objednateli. Nad rámec požadavků specifikovaných níže musí plnění Zhotovitele splňovat veškeré požadavky stanovené ve Smlouvě a jejích přílohách, přičemž nesplnění kterékoliv z nich může být důvodem, který Objednatele opravňuje odmítnout předání a převzetí příslušné části Díla.

Etapa	Název	Předmět plnění	Požadavky na podobu předávané části Díla	Způsob prokázání úplnosti části Díla
1	Projektování	Zpracování a schválení prováděcího projektu	Projekt bude zpracován na základě analýzy aktuálního stavu v prostředí Zadavatele Projekt bude obsahovat detailní Prováděcí projekt dodávaného systému Projekt bude obsahovat návrh procesu předání a akceptace díla, vč. návrhu protokolů	Výsledný Prováděcí projekt musí být schválen ze strany Zadavatele Schválení Prováděcího projektu Zadavatelem bude podmiňovat zahájení Etapy2
		Příprava testovacího prostředí	Příprava technických podmínek pro vývoj a testování, vč. <i>vytvoření Metodiky testování</i> , pro budoucí testování dodávaného díla v Etapě 3.	Souhlasné vyjádření dodavatele platební brány Schválení Metodiky testování Zadavatelem bude podmiňovat zahájení Etapy2

		Zajištění vybavení a součinnosti zadavatele	Požadavky na součinnost Zadavatele nad rámec závazku daných Zadávací dokumentací musí být formulovány Dodavatelem do Prováděcího projektu	
		Zajištění vybavení a součinnosti dopravců	Požadavky na součinnost dalších subjektů musí být formulovány Dodavatelem do Prováděcího projektu	
2	Vývoj a implementace	Vývoj základního jádra zúčtovacího systému	Vývoj a implementace předávaného díla plně ve shodě s Prováděcím projektem	Základní funkční test posuzující, zda předávaná část díla neobsahuje zjevné nedodělky a vady
		Vývoj mobilní aplikace		dtto
		Vývoj webové aplikace		dtto
		Vývoj revizorského systému		dtto
		Implementace zadané platební brány		Vyjádření o funkčnosti dodavatelem platební brány
		Instalace HW a SW do prostředí Kraje Vysočina (zadavatele)		Vyjádření příslušného odboru zadavatele

		Vývoj SW pro předprodeje dopravců		Základní funkční test posuzující, zda předávaná část díla neobsahuje zjevné nedodělky a vady
3	Testování	Testování dílčích částí systému dodavatelské testy	Testy dle Metodiky testování (provedení penetračních/zátěžových testů) Předání aktualizovaného prováděcího projektu včetně dokumentace skutečného provedení díla.	Akceptace díla, jako celku na základě: a) Úspěšných výsledků testování b) Úspěšného pilotního provozu
		Beta testování u zadavatele		
		Pilotní provoz		
		Zahájení rutinního provozu	Zahájení celoplošného uplatnění EOC ve VDV	

Akceptace/předání dílčích částí Díla definovaných pro dodávku systému bude potvrzena podpisem dílčích předávacích a akceptačních protokolů.

Po akceptaci/předání dílčích částí Díla definovaných pro dodávku systému bude zahájen jejich provoz s tím, že Zhotovitel je povinen provádět údržbu a podporu akceptovaných dílčích částí Díla za podmínek, které budou stanoveny v Servisní smlouvě.

Příloha č. 3
Smlouvy o dílo

Seznam Poddodavatelů

PODDODAVATEL Č. 1	
Jméno poddodavatele <i>(název, obchodní firma, příp. jméno a příjmení)</i>	ODP-software, spol. s r.o.
IČO	61683809
Sídlo / místo podnikání / bydliště	Pernerova 2819/2a, Žižkov, 130 00 Praha 3
Část veřejné zakázky, kterou bude poddodavatel plnit	1. Systém mobilních zařízení pro revizory – dle kapitoly 8 přílohy č. 4 Dokumentace zadávacího řízení, včetně dodávky HW mobilních zařízení pro revizory. 2. Mobilní aplikace systému elektronického odbavení cestujících dle kapitoly 13 přílohy č. 4 Dokumentace zadávacího řízení, včetně vyhledávače trasy s rozhraním pro využití v e-shopu dle kapitoly 5.5.3 přílohy č. 4 Dokumentace zadávacího řízení a kalkulátoru jízdného s rozhraním pro využití v e-shopu dle kapitoly 5.5.2 přílohy č. 4 Dokumentace zadávacího řízení. 3. Prodejní portál (prodejní místo –předprodej u dopravce) – dle kapitoly 7 přílohy č. 4 Dokumentace zadávacího řízení.
Podíl části veřejné zakázky, jež bude poddodavatel plnit v Kč bez DPH nebo % z nabídkové ceny	46 %

Příloha č. 4
Smlouvy o dílo

Seznam členů realizačního týmu

MANAŽER PROJEKTU	
Titul, jméno a příjmení (titul, jméno a příjmení)	

SYSTÉMOVÝ ARCHITEKT	
Titul, jméno a příjmení (titul, jméno a příjmení)	

PRACOVNÍK VÝVOJE SOFTWARE	
Titul, jméno a příjmení (titul, jméno a příjmení)	

Příloha č. 5
Smlouvy o dílo

Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele

1. Základní bezpečnostní požadavky

- **Bezpečnost přístupových oprávnění zhotovitele**
 - Zhotovitel je povinen chránit veškeré své přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům zhotovitele, které umožňují přístup k informačním aktivům objednatele či umožňují jejich správu.
 - Zhotovitel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
 - min. délka hesla 17 znaků
 - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
 - malá písmena
 - velká písmena
 - číslice
 - speciální znaky
 - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě
 - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
 - platnost hesla musí být maximálně 1,5 roku.
 - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
 - Pokud by Zhotovitel zřizoval přístupová oprávnění třetí straně, je Zhotovitel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.
- **Řízení rizik**
 - Objednatel si vyhrazuje právo na informace o tom, jakým způsobem zhotovitel řídí rizika v souvislosti s plněním této smlouvy, tedy o tom, jakou metodiku pro řízení rizik používá, jakým způsobem jsou rizika hodnocena a klasifikována, jakým způsobem jsou rizika ošetřována a kdo je za řízení rizik za zhotovitele zodpovědný.
 - Zhotovitel se zavazuje řídit rizika informační bezpečnosti minimálně v následujícím rozsahu:
 - Identifikace a ohodnocení aktiv souvisejících s plněním této smlouvy,
 - Identifikace, analýza a ohodnocení rizik souvisejících s plněním této smlouvy,
 - Zvládání a monitoring rizik souvisejících s plněním této smlouvy.
- **Řízení kybernetických bezpečnostních incidentů:**
 - Zhotovitel je povinen objednateli transparentně a pravdivě hlásit veškeré kybernetické bezpečnostní incidenty, které by mohli mít nějakou souvislost s:
 - informačními aktivy objednatele,
 - přístupovými údaji k informačním aktivům objednatele,
 - informacemi objednatele.
 - Zhotovitel je povinen výše zmíněné kybernetické bezpečnostní incidenty evidovat.
 - Zhotovitel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy objednatele.
- **Bezpečné vývojové prostředí**
 - Níže uvedené požadavky týkající se zdrojového kódu budou aplikovány na zdrojový kód, jehož autorem je Zhotovitel.
 - Zhotovitel je povinen zajistit ochranu před škodlivým kódem:
 - na pracovních stanicích svých vývojářů a programátorů,
 - na serverech/zařízeních, kde je uložen zdrojový kód Díla.

- Zhotovitel je povinen řídit přístup ke zdrojovým kódům tak, aby k němu měli přístup pouze oprávnění vývojáři a jiné oprávněné osoby Zhotovitele.
- Zhotovitel musí přístupy ke zdrojovým kódům a jejich změny monitorovat a zaznamenávat, auditní stopu přístupů musí vyhodnocovat. Pro správu zdrojového kódu musí být použit tzv. verzovací systém.
- Zhotovitel je povinen zdrojové kódy díla pravidelně zálohovat a zálohy pravidelně testovat na jejich obnovitelnost.

2. Zvýšené bezpečnostní požadavky

Zvýšené bezpečnostní požadavky uvedené níže se týkají pouze funkcionalit systému EOC

vyjmenovaných v kapitole 12.2 *Speciální požadavky na návrh systému* dokumentu 04.0 -Příloha č.4 DZŘ

- Zhotovitel je povinen používat personifikované účty s výjimkou systémových či technických účtů sloužících pro běh programového vybavení, přičemž tyto systémové účty neumožňují interaktivní přihlášení. Výše uvedené personifikované účty musí být nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
- Kryptografie
 - Zhotovitel je povinen u veškerých kryptografických funkcí a metod souvisejících s plněním této smlouvy dodržovat minimální požadavky, které jsou stanoveny takto:

Kryptografie obecně

Pro šifrování, elektronické podepisování a provádění otisků dat (hashování) nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejich funkcionalita je všeobecně známá a popsána.

Hashovací funkce

Ukládání otisků hesel

- pro ukládání hesel personifikovaných, nesystémových uživatelů ukládaných v rámci Díla mohou být použity pouze tyto tzv. pomalé hashovací funkce:
 - Argon2i
 - bcrypt
 - scrypt
 - PBKDF2
- při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt
- pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

Elektronické podepisování e-mailů a dokumentů

- SHA-2 a vyšší
- délka otisku 256 bitů a vyšší

Ověřování integrity souborů

- SHA-2 a vyšší
- délka otisku 224 bitů a vyšší

Asymetrická kryptografie

SSL/TLS

- verze protokolu minimálně TLSv1.2 a vyšší
- konfigurace
 - cipher suite musí být vybrána na základě serverem preferovaného pořadí
 - vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:
 - ECDHE musí mít vyšší prioritu než DHE
 - ECDSA musí mít vyšší prioritu než DSA
 - všechny EXPORT cipher suites musí být zakázány
 - algoritmy a funkce pro výměnu klíčů
 - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
 - tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
 - a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn., že pro každou session je generován nový set Diffie-Hellman klíčů
 - délky klíčů:
 - pro Diffie-Hellman (DH) - 2048 bitů a více (postupně přecházet na 3072 bitů, tam kde to bude možné)
 - pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
 - nesmí být použita anonymní výměna klíčů
 - algoritmy a funkce pro autentizaci
 - minimální délky klíčů:
 - RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
 - ECDSA - 256 bitů
 - algoritmy a funkce pro symetrické šifrování
 - nesmí být použita hodnota NULL v cipher suites
 - nesmí být použity tyto šifry:
 - DES, 3DES, RC4
 - minimální délka šifrovacího klíče - 128 bitů
 - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
 - MAC (Message Authentication Code)
 - použití SHA funkce s minimální délkou hashe 256 bitů
 - vyšší délky otisků musí mít vyšší prioritu v cipher suites
- Certifikáty dodá zadavatel

TLS cipher suites

- Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
- TLS1.3:
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_128_CCM_SHA256
- TLS1.2:
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
 - algoritmus DSA – 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
 - algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
 - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
 - délka klíče minimálně 2048 bitů u RSA a DSA algoritmů (postupně přecházet na 3072 bitů, tam kde to bude možné)
 - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

Symetrická kryptografie

- nesmí být použity tyto šifry:
 - DES, 3DES, RC4, Blowfish, Kasumi
- minimální délka šifrovacího klíče - 128 bitů
 - pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
- nesmí být použity tyto módy pro ochranu integrity:
 - HMAC-SHA1, CBC-MAC-X9.19