



KUMSP002K8H4

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační programMINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

MORAVSKOSLEZSKÝ KRAJ – KRAJSKÝ ÚŘAD

ČÍSLO SMLOUVY (DODATKU)

-1-

0426P

poř. číslo

2014

rok

INF

zkr. odb.

SMLOUVA

na zajištění Správy identit krajské korporace

I.

Smluvní strany

1. Moravskoslezský kraj

Se sídlem: 28. října 117, 702 18 Ostrava
Zastoupen: prof. Ing. Ivo Vondrákem, CSc., hejtmanem kraje
IČ: 70890692
DIČ: CZ70890692
Bankovní spojení: Česká spořitelna, a.s.
Číslo účtu: 200184-1650676349/0800

(dále jen „objednatel“)

a

2. NEWPS.CZ s.r.o.

Se sídlem: Přemyslovská 2845/43, 130 00 Praha 3
Zastoupena: Ing. Martinem Řehořkem
IČ: 25625632
DIČ: CZ25625632
Bankovní spojení: Raiffeisenbank a.s., Hvězdova 1716/2b, 140 78 Praha 4
Číslo účtu: 5081103433/5500
Zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 55889

(dále jen „zhotovitel“)

II.

Základní ustanovení

1. Tato smlouva je uzavřena dle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“); práva a povinnosti stran touto smlouvou neupravená se řídí příslušnými ustanoveními občanského zákoníku.
2. Smluvní strany prohlašují, že údaje uvedené v čl. I této smlouvy jsou v souladu se skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení písemně druhé smluvní straně. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek.
3. Je-li zhotovitel plátcem DPH, prohlašuje, že bankovní účet uvedený v čl. I odst. 2 této smlouvy je bankovním účtem zveřejněným ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“). V případě změny účtu zhotovitele je zhotovitel povinen doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu; je-li zhotovitel plátcem DPH, musí být nový účet zveřejněným účtem ve smyslu předchozí věty.

4. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto jednání oprávněny.
5. Zhotovitel prohlašuje, že je odborně způsobilý k zajištění předmětu plnění podle této smlouvy.
6. Plnění této smlouvy je realizováno v rámci projektu „Rozvoj architektury ICT Moravskoslezského kraje“ v rámci Integrovaného regionálního operačního programu (dále jen „IROP“), prioritní osa 3. Dobrá správa území a zefektivnění veřejných institucí, výzva č. 28, Specifické informační a komunikační systémy a infrastruktura II. Zhotovitel je povinen postupovat v souladu s pravidly IROP a výzvou k předkládání žádostí o podporu relevantní pro tento projekt. Tyto dokumenty jsou dostupné na webových stránkách: <http://www.strukturalni-fondy.cz>.
7. Účelem této smlouvy je podpořit centralizaci a standardizaci správy identit pro krajský úřad a příspěvkové organizace Moravskoslezského kraje (dále také „MSK“).

III. Předmět smlouvy

1. Zhotovitel je povinen provést na svůj náklad a nebezpečí pro objednatele zajištění rozšíření stávajících prostředků a funkcionalit systému pro správu identit Krajského úřadu Moravskoslezského kraje tak, aby byly pokryty veškeré plánované aktivity související s rozvojem sdílených služeb a rozšířit využívání technologie identity managementu (IDM) v ICT vybraných příspěvkových organizacích Moravskoslezského kraje (lokální IDM, integrace významných systémů organizace, napojení na Active Directory, bezpečná autentizace, synchronizace s JIP, podpora eIDAS atd.) (dále jen „dílo“).
2. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro objednatele níže specifikované dílo ve dvou dílčích plněních, a to:

2.1 Realizace díla, spočívající v provedení následujících částí díla:

- a) **Rozšíření stávajících licencí na geografickou multilicenci PUMA IAM Advanced Edition** pro neomezený počet uživatelů v rámci Moravskoslezského kraje.
- b) Zpracování a předání **analýzy a prováděcího návrhu úprav a rozvoje systému správy identit** v rozsahu dle technické specifikace uvedené v příloze č. 1 této smlouvy.
- c) **Úprava portálu samoobslužného řešení.**
- d) **Rozšíření IDM o workflow modul.**
- e) Systém zasílání logů do SIEM
- f) Typová instalace a konfigurace otevřeného vzorového konektoru (vzor pro HR systémy).
- g) Specifikace integračního rozhraní pro integraci aplikací.
- h) Úprava systému rolí, propagace rolí.
- i) Škálování AGW pro vyšší výkon a dostupnost.
- j) Vývoj autentizační metody podle specifikace EIDAS do AGW.

k) Vytvoření testovacího prostředí.

l) Customizace auditních reportů.

2.2 Provozní část díla (rutinní provoz)

m) Technická podpora.

n) Další služby (Školení, Konzultační práce, Programátorské práce).

3. Objednatel se zavazuje provedené dílo převzít a zaplatit za ně zhotoviteli cenu podle čl. VI této smlouvy.

IV.

Vymezení pojmů a zkratek

1. Smluvní strany se pro účely této smlouvy dohodly na následujícím vymezení pojmů:

- pod pojmem *Technologické centrum kraje* se rozumí datové centrum Krajského úřadu Moravskoslezského kraje,
- pod pojmem *Realizace díla* se rozumí provádění částí díla uvedených v čl. III odst. 2.1 této smlouvy zhotovitelem. Realizace díla je ukončena předáním a převzetím poslední části díla bez vad a nedodělků,
- pod pojmem *Provozní část díla (rutinní provoz)* se rozumí bezchybné a komplexní fungování díla po dobu 60 měsíců, které započne po předání a převzetí poslední z částí díla uvedených v čl. III odst. 2.1 této smlouvy (vyjma část uvedené pod písm. j) odst. 2 článku V),
- pod pojmem *Technická podpora* se rozumí poskytování služeb dle Přílohy č. 2 této smlouvy,
- pod pojmem *geografická multilicence* se rozumí multilicence definovaná v kap. 5 Přílohy č. 1 – Technická specifikace.

2. Smluvní strany se pro účely této smlouvy dohodly na následujícím vymezení zkratek:

- IDM MSK – systém pro správu identit
- MSK – Moravskoslezský kraj
- krajská korporace – příspěvková organizace zřízená Moravskoslezským krajem
- KÚ MSK – Krajský úřad Moravskoslezského kraje

V.

Místo předání a doba plnění

1. Zhotovitel je povinen předat objednateli dílo v místě předání, kterým je budova Krajského úřadu Moravskoslezského kraje, 28. října 117, 702 18 Ostrava.

2. Zhotovitel je povinen části díla provést a předat objednateli bez vad a nedodělků v těchto termínech:

- a) Rozšíření stávajících licencí na **geografickou multilicenci PUMA IAM Advanced Edition** pro neomezený počet uživatelů v rámci Moravskoslezského kraje a zajištění

1000 licencí pro uživatele mimo region Moravskoslezského kraje do **1 měsíce** ode dne nabytí účinnosti smlouvy.

- b) Zpracování a předání **Analýzy a prováděcího návrhu úprav a rozvoje systému správy identit** v rozsahu dle technické specifikace uvedené v příloze č. 1 této smlouvy do **4 měsíců** ode dne nabytí účinnosti smlouvy.
 - c) Úprava portálu samoobslužného řešení do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - d) Rozšíření IDM o workflow modul do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - e) Systém zasílání logů do SIEM do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - f) Typová instalace a konfigurace otevřeného vzorového konektoru (vzor pro HR systémy) do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - g) Specifikace integračního rozhraní pro integraci aplikací do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - h) Úprava systému rolí, propagace rolí do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - i) Škálování AGW pro vyšší výkon a dostupnost do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - j) Vývoj autentizační metody podle specifikace EIDAS do AGW do **12 měsíců** ode dne výzvy objednatele, která může být učiněna nejdříve po zveřejnění podmínek pro připojení ke službám národní identitní autority (NIA) pro poskytovatele služeb ze strany orgánů veřejné moci publikovaných na stránkách Správy základních registrů <http://www.szrcr.cz>. Ověření zveřejněné dokumentace u SZR je povinen zajistit objednatel a předat tuto informaci zhotoviteli. Objednatel však není povinen, ani při naplnění podmínek uvedených výše, tuto výzvu učinit. Učinění či neučinění této výzvy nemá vliv na ostatní termíny a rozsah plnění uvedený v této Smlouvě. Zhotovitel bere na vědomí, že tato část díla se nebude realizovat v případě, že objednatel nezašle výzvu ani do 31. 12. 2018.
 - k) Vytvoření testovacího prostředí do **12 měsíců** ode dne nabytí účinnosti smlouvy.
 - l) Customizace auditních reportů do **12 měsíců** ode dne nabytí účinnosti smlouvy.
3. Zhotovitel bere na vědomí a souhlasí s tím, že Technickou podporu bude poskytovat po celou dobu účinnosti smlouvy, tj. po dobu Realizace díla a trvání rutinního provozu.
4. Zhotovitel bere na vědomí a souhlasí s tím, že Další služby (Školení, Konzultační práce, Programátorské práce) bude poskytovat po celou dobu účinnosti smlouvy, a to vždy na základě požadavku (jednotlivých objednávek) objednatele.
5. Dílo je provedeno, je-li dokončeno a předáno objednateli. Smluvní strany se dohodly, že objednatel není povinen dílo převzít, pokud toto vykazuje vady či nedodělky.

VI. Cena

1. Cena za dílo je stanovena v příloze č. 3 této smlouvy.

2. Zhotovitel bere na vědomí a výslovně souhlasí s tím, že Technická podpora v době realizace

díla dle čl. III odst. 2.1 této smlouvy bude poskytována bezplatně.

3. Cena za dílo zahrnuje veškeré náklady zhotovitele spojené se splněním jeho závazku z této smlouvy, tj. cenu díla včetně dopravného, odměny za poskytnutí licence, nákladů spojených s publicitou projektu, nákladů na veškeré instalační práce apod. Cena za dílo je stanovena jako nejvýše přípustná a není ji možno překročit.
4. Je-li zhotovitel plátcem DPH, odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy; v případě, že dojde ke změně zákonné sazby DPH, je zhotovitel k ceně díla bez DPH povinen účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny díla v důsledku změny sazby DPH není nutno k smlouvě uzavírat dodatek. V případě, že zhotovitel stanoví sazbu DPH či DPH v rozporu s platnými právními předpisy, je povinen uhradit objednateli veškerou škodu, která mu v souvislosti s tím vznikla.

VII.

Předání díla, vlastnické právo k předmětu díla a nebezpečí škody

1. Objednavatel se zavazuje předat objednateli samostatně část díla dle čl. V odst. 2.1 písm. a) této smlouvy. Dále se zavazuje předat samostatně objednateli části díla dle čl. V odst. 2.1 c) – l) této smlouvy (vyjma část pod písm. j, která bude v případě realizace předána rovněž samostatně). O předání a převzetí částí díla zhotovitel sepíše bezodkladně **Předávací protokol**, ve kterém objednatel prohlásí, zda část díla přijímá či nikoli.
2. Objednatel je povinen předat objednateli část díla dle čl. V odst. 2.1 písm. b) této smlouvy objednateli ke schválení a případnému zapracování připomínek k prováděcímu návrhu úprav a rozvoje systému správy identit. Zhotovitel si k prostudování, připomínkování a schválení podoby uvedené části díla vyhrazuje **10 pracovních dnů**. Zhotovitel bere na vědomí, že doba plnění této části díla uvedená v čl. V odst. 2 písm. b) této smlouvy není tímto ustanovením nijak dotčena. O předání a převzetí části díla zhotovitel sepíše bezodkladně **Předávací protokol**, ve kterém objednatel prohlásí, zda část díla přijímá či nikoli.
3. Pokud objednatel dílo nebo jeho část nepřevzme, protože obsahuje vady či nedodělky, je povinen specifikovat tyto vady v předávacím protokolu.
4. Dílo a jeho části dle čl. III odst. 2 této smlouvy přebírá objednatel prostřednictvím pověřených osob z odboru informatiky KÚ MSK.
5. Zhotovitel a objednatel jsou oprávněni uvést v předávacím protokolu cokoliv, co budou považovat za nutné.
6. Předávací protokol musí obsahovat minimálně tyto náležitosti:
 - a) číslo Předávacího protokolu a datum jeho vyhotovení,
 - b) číslo smlouvy a datum jejího uzavření, číslo veřejné zakázky (tj. 59/2017).
 - c) označení předmětu plnění (resp. dílo a jeho části) v souladu s členěním dle čl. III odst. 2 této smlouvy vč. soupisu dodaných jednotlivých položek a provedených prací na díle, odpovídající jednoznačně jak obsahem, tak formátem technickým podmínkám a specifikacím dle členění smlouvy.
 - d) název, sídlo, IČ a DIČ objednatele a zhotovitele,
 - e) prohlášení objednatele, že dílo nebo jeho část přijímá či nikoliv a prohlášení zhotovitele, že předané dílo nebo jeho část je bez vad a nedodělků a plně funkční; pokud dílo nebo jeho část nebude objednatelem převzato, bude protokol obsahovat

specifikaci vad díla či jeho části,

- f) jméno, vlastnoruční podpis, kontaktní telefon a e-mail zástupců objednatele a zástupců zhotovitele,
- g) datum předání a převzetí díla (každé dílčí části vč. označení doby začátku a konce prací či dodávky).

7. Vlastnické právo k věci, která je předmětem díla (jeho dílčí části) a nebezpečí škody na ní přechází na objednatele dnem převzetí díla objednatelem.

VIII.

Platební a fakturační podmínky

1. Úhrada ceny za **realizaci části díla** dle čl. III odst. 2.1 písm. **a)** této smlouvy bude provedena po předání a převzetí této části díla bez vad a nedodělků.
2. Úhrada ceny za **realizaci částí díla** dle čl. III odst. 2.1 písm. **b) – i) a k) – l)** této smlouvy bude provedena současně po úspěšném předání a převzetí poslední z uvedených částí díla bez vad a nedodělků.
3. Úhrada ceny za realizaci části díla dle čl. III odst. 2.1 písm. **j)** této smlouvy bude provedena po úspěšném předání a převzetí části díla bez vad a nedodělků.
4. Úhrada ceny za **Technickou podporu** dle čl. III odst. 2.2 této smlouvy bude prováděna zpětně za období jednoho roku poskytování Technické podpory, počítáno ode dne předání a převzetí poslední části díla bez vad a nedodělků, a to bez ohledu na případnou realizaci části díla dle čl. III odst. 2.1 písm. **j)** této smlouvy.
5. Úhrada ceny za **Další služby** dle čl. III odst. 2.2 této smlouvy bude prováděna jednotlivě po provedení těchto služeb.
6. Zálohové platby nebudou poskytovány.
7. Podkladem pro úhradu ceny za dílo budou faktury, které budou mít náležitosti daňového dokladu dle zákona o DPH a náležitosti stanovené dalšími obecně závaznými právními předpisy. Není-li zhotovitel plátcem DPH, podkladem pro úhradu ceny za dílo bude faktura, která bude mít náležitosti účetního dokladu dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a náležitosti stanovené dalšími obecně závaznými právními předpisy.
8. Faktury musí dále obsahovat:
 - a) číslo smlouvy objednatele, číslo veřejné zakázky (tj. 59/2017), IČ objednatele,
 - b) označení předmětu plnění v souladu s členěním dle čl. III odst. 2 této smlouvy
 - c) označení banky a číslo účtu, na který musí být zapláceno (pokud je číslo účtu odlišné od čísla uvedeného v čl. I odst. 2, je zhotovitel povinen o této skutečnosti v souladu s čl. II odst. 3 této smlouvy informovat objednatele),
 - d) lhůtu splatnosti faktury,
 - e) označení osoby, která fakturu vyhotovila, včetně jejího podpisu, kontaktního telefonu a e-mailu,
 - f) číslo a datum předávacího protokolu podepsaného oběma smluvními stranami (předávací protokol obsahující prohlášení objednatele, že plnění přejímá, bude přílohou faktury),
 - g) označení odboru, který akci likviduje (odbor evropských projektů po dobu realizace

díla; po dobu rutinního provozu odbor informatiky),

- h) název a registrační číslo projektu: „Rozvoj architektury ICT Moravskoslezského kraje“, reg. č. CZ.06.3.05/0.0/0.0/16_044/0002010, spolufinancovaný v rámci Integrovaného regionálního operačního programu,
- i) přílohou faktury za realizaci díla dle odst. 1 a odst. 2 tohoto článku bude kopie předávacího protokolu s náležitostmi dle čl. VII odst. 6 této smlouvy.
9. Povinnost zaplatit cenu za dílo je splněna dnem odepsání příslušné částky z účtu objednatele.
10. Lhůta splatnosti faktury je dohodou stanovena na 30 kalendářních dnů ode dne jejího doručení objednateli. Doručení faktury se provede osobně oproti podpisu zmocněné osoby objednatele nebo doručenkou prostřednictvím provozovatele poštovních služeb nebo do datové schránky.
11. Přílohou faktury za realizaci díla bude podrobný rozpis ceny předmětu plnění za účelem evidence majetku a jeho odepisování dle zákona č. 586/1992 Sb., o daních z příjmu, ve znění pozdějších předpisů, a zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. U dlouhodobého hmotného a nehmotného majetku bude uveden klasifikační kód CZ-CPA za účelem odepisování dlouhodobého hmotného a nehmotného majetku.
12. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy s vyznačením důvodu vrácení. Zhotovitel provede opravu vystavením nové faktury. Vrácením vadné faktury zhotoviteli přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne doručení nové faktury objednateli.
13. Objednatel, příjemce plnění, prohlašuje, že plnění, které je předmětem smlouvy, nepoužije pro svou ekonomickou činnost, ale výlučně pro účely související s jeho činností při výkonu veřejné správy, při níž se nepovažuje za osobu povinnou k dani (viz § 5 odst. 3 zákona o DPH). Z uvedeného důvodu se na toto plnění nevztahuje režim přenesení daňové povinnosti dle příslušných ustanovení uvedeného zákona a zhotovitelem, je-li plátcem DPH, bude vystavena faktura za zdanitelné plnění včetně daně z přidané hodnoty.
14. Je-li zhotovitel plátcem DPH, objednatel uplatní institut zvláštního způsobu zajištění daně dle § 109a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uvedené na faktuře uhradí v termínu splatnosti této faktury stanoveném dle smlouvy přímo na osobní depozitní účet zhotovitele vedený u místně příslušného správce daně v případě, že:
- a) zhotovitel bude ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr plátců DPH“ jako nespolehlivý plátc, nebo
 - b) zhotovitel bude ke dni uskutečnění zdanitelného plnění v insolvenčním řízení, nebo
 - c) bankovní účet zhotovitele určený k úhradě plnění uvedený na faktuře nebude správcem daně zveřejněn v aplikaci „Registr plátců DPH“.

Objednatel nenese odpovědnost za případné penále a jiné postihy vyměřené či stanovené správcem daně zhotoviteli v souvislosti s potenciálně pozdní úhradou DPH, tj. po datu splatnosti této daně.

IX.

Práva a povinnosti smluvních stran

1. Není-li stanoveno touto smlouvou výslovně jinak, řídí se vzájemná práva a povinnosti smluvních stran ustanoveními § 2586 a následujícími občanského zákoníku.
2. Zhotovitel je zejména povinen:
 - a) Provést dílo (díličí část) řádně a včas za použití materiálu a postupů odpovídajících

právním předpisům a technickým normám ČR. Smluvní strany se dohodly na I. jakosti díla (nové, nerepasované apod.). Dílo musí odpovídat příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se k provedení díla a umožňovat užívání, k němuž bylo určeno a zhotoveno.

- b) Řídit se při provádění díla pokyny objednatele a aktuální Bezpečnostní politikou Krajského úřadu, k níž bude zhotovitel proškolen objednatelem bezprostředně po nabytí účinnosti této smlouvy.
 - c) Umožnit objednateli kontrolu provádění díla kdykoliv v průběhu plnění smlouvy. Pokud objednatel zjistí, že zhotovitel neprovádí dílo řádně či jinak porušuje svou povinnost, poskytne zhotoviteli lhůtu k nápravě; neučiní-li tak zhotovitel ve stanovené lhůtě, je objednatel oprávněn od smlouvy odstoupit.
 - d) Odstranit zjištěné vady a nedodělky na své náklady.
 - e) Dbát při provádění díla dle této smlouvy na ochranu životního prostředí a dodržovat platné technické, bezpečnostní, zdravotní, hygienické a jiné předpisy, včetně předpisů týkajících se ochrany životního prostředí.
 - f) Postupovat při provádění díla s odbornou péčí.
 - g) Uchovávat veškerou dokumentaci související s realizací předmětu plnění dle této smlouvy včetně účetních dokladů minimálně do konce roku 2028, není-li v českých právních předpisech stanovena lhůta delší.
 - h) Minimálně do konce roku 2028 poskytovat požadované informace a dokumentaci související s realizací plnění zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, 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 plnění a poskytnout jim při provádění kontroly součinnost.
 - i) Zhotovitel je povinen se řídit pravidly pro publicitní opatření výzvy a projektu, dostupných na <http://www.strukturalni-fondy.cz>.
 - j) Zhotovitel je povinen postupovat v souladu s pokyny poskytovatele dotace, které jsou pro něj relevantní ve vztahu k projektu. Pokyny jsou dostupné také na <http://www.strukturalni-fondy.cz>.
 - k) Umístit prvky publicity jako součást poskytnuté aplikace/software v rámci provedeného díla, bude-li to informační prostřední umožňovat.
3. V rámci kontrolních oprávnění objednatele dle čl. IX odst. 2 písm. c) této smlouvy bude objednatel organizovat ve svém sídle (neurčí-li objednatel výslovně jinak) pravidelné kontrolní dny, které budou probíhat ode dne, kdy smlouva nabude účinnosti, a to v následujících intervalech:
- a) v průběhu realizace díla jedenkrát měsíčně,
 - b) v průběhu rutinního provozu jedenkrát za čtvrtletí, nedohodnou-li se smluvní strany jinak.

Zhotovitel je povinen zajistit účast zástupce jeho realizačního týmu na kontrolních dnech.

Objednatel může dle aktuální potřeby frekvenci konání těchto kontrolních dní upravit.

4. Zhotovitel je povinen účastnit se na základě pozvánky objednatele všech jednání týkajících se předmětu smlouvy, řídit se při provádění plnění dle této smlouvy jeho pokyny a poskytnout mu požadovanou dokumentaci. Účast na těchto jednáních není považována za technickou podporu, údržbu, poradenství ani konzultaci a zhotoviteli za takové jednání nenáleží odměna.
5. Zhotovitel je povinen z každého jednání dle předchozího odstavce a z každého kontrolního dne týkajícího se plnění předmětu smlouvy vyhotovit zápis o průběhu a závěrech jednání dle předchozího odstavce či kontrolního dne, který bude v případě odsouhlasení podepsán zástupci objednatele i zhotovitele, a to bezprostředně po takovémto jednání a současně odeslán na e-mail objednatele nebo bude objednateli předán jinou obdobnou formou. Každý ze zápisů bude obsahovat minimálně tyto náležitosti: pořadové číslo zápisu, datum konání, místo konání, seznam přítomných či omluvených účastníků, program jednání, popis sjednaných úkolů a závěrů jednání dle předchozího odstavce či kontrolního dne; popis splnění úkolů ujednaných na předchozím jednání dle předchozího odstavce či předchozím kontrolním dni; název projektu, reg. číslo projektu a prvky povinné publicity dle čl. IX odst. 2 písm. i) této smlouvy. Objednatel si vyhrazuje právo zápis nepřevzít, nepodepsat a prohlásit jej vadným, nebude-li obsahovat některý z výše uvedených údajů.
6. Zhotovitel je povinen v průběhu Realizace díla i v průběhu Rutinního provozu předat či zaslat v písemné podobě (elektronicky na určený e-mail objednatele) Zprávu o pokroku prací (tj. popis činností, jež zhotovitel za předcházející období provedl v souvislosti s realizací předmětu plnění). Zpráva o pokroku prací bude obsahovat název projektu, reg. číslo projektu a prvky povinné publicity dle odst. IX čl. 2 písm. i) této smlouvy, pořadové číslo zprávy, datum, jméno a podpis pověřené osoby. Objednatel si vyhrazuje právo Zprávu o pokroku prací nepřevzít a prohlásit ji za vadnou, nebude-li obsahovat některý z výše uvedených údajů. Zpráva o pokroku prací bude předána vždy nejpozději do 1 měsíce ode dne, kdy objednatel vyzve zhotovitele k zaslání této zprávy. Taková zpráva bude obsahovat popis provedených činností na díle za období zvolené objednatel.
7. Objednatel je zejména povinen poskytnout zhotoviteli součinnost nutnou k provedení díla a plnit povinnosti dle odst. 2 písm. j) předchozího článku smlouvy.
8. Smluvní strany berou na vědomí, že předmět díla bude možné také realizovat prostřednictvím vzdáleného přístupu do datové sítě zhotovitele protokolem TCP/IP, a to v souladu s pravidly definovanými v aktuální bezpečnostní politice objednatele, se kterou bude zhotovitel seznámen objednatel.
9. Seznam poddodavatelů uvede zhotovitel v příloze č. 4 této smlouvy. Zhotovitel je povinen písemně informovat objednatele o všech dalších (nových) poddodavatelích (včetně jejich identifikačních a kontaktních údajů a o tom, které služby pro něj v rámci předmětu plnění každý z poddodavatelů poskytuje) a o jejich změně, a to nejpozději do 7 kalendářních dnů ode dne, kdy zhotovitel vstoupil s poddodavatelem ve smluvní vztah či ode dne, kdy nastala změna. Zhotovitel je oprávněn změnit poddodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení, na základě něhož byla uzavřena tato smlouva, jen z vážných objektivních důvodů a s předchozím písemným souhlasem objednatele, přičemž nový poddodavatel musí disponovat kvalifikací ve stejném či větším rozsahu, který původní poddodavatel prokázal za zhotovitele.
10. Zhotovitel objednateli odpovídá za to, že dokumenty a soubory dat, které mu v rámci plnění předmětu smlouvy předal:
 - a) Jsou autorizovanými kopiemi originálů příslušných dokumentů a souborů dat

zhotovitele,

- b) neobsahují žádné infiltrační prostředky,
- c) že k nim má práva na jejich šíření, instalaci, konfiguraci a správu, která mu umožňují s nimi nakládat a dále je poskytovat tak, jak je sjednáno v této smlouvě.

11. Objednatel má právo vyjadřovat připomínky k plnění předmětu smlouvy zhotovitelem, a to i opakovaně. Zhotovitel je povinen tyto připomínky zohlednit.

X.

Zaměstnanci a poddodavatelé zhotovitele a osoby zúčastněné na plnění předmětu smlouvy v jiném právním vztahu ke zhotoviteli

1. Zhotovitel prohlašuje, že všichni jeho pracovníci, kteří se budou podílet na realizaci předmětu plnění, mají dostatečnou kvalifikaci v oboru.
2. Zhotovitel zajistí, aby jeho pracovníci, kteří budou přítomni v prostorách objednatele, dodržovali všechny bezpečnostní předpisy tak, jak s nimi byli seznámeni objednatelem.

XI.

Oznámení a komunikace

1. Veškerá komunikace na základě této smlouvy bude probíhat v souladu s tímto článkem. Kromě jiných způsobů komunikace dohodnutých mezi stranami se za účinné považují osobní doručování, doručování doporučenou poštou, datovou schránkou, či elektronickou poštou, a to na adresy smluvních stran, nebo na takové adresy, které si strany vzájemně písemně oznámí. Kontaktní údaje je možné nahlásit na kontrolních dnech, kde se tato skutečnost napíše do zápisu.
2. Oznámení správně adresovaná se považují za uskutečněná v případě osobního doručování anebo doručování doporučenou poštou okamžikem doručení, v případě posílání elektronickou poštou okamžikem obdržení potvrzení od protistrany při použití stejného komunikačního kanálu.
3. Informace a materiály, které obsahují osobní údaje a důvěrné informace budou doručovány buď osobně, nebo zasílány elektronickou poštou a šifrovány. Šifra pro elektronickou poštu bude určena před zahájením prací.

XII.

Licenční ujednání

1. Zhotovitel poskytuje touto smlouvou objednateli a objednatel touto smlouvou přijímá nevýhradní oprávnění k užití software dodávaného jako součást díla, a to všemi způsoby uvedenými v ust. § 12 odst. 4 autorského zákona.
2. Zhotovitel poskytne objednateli veškeré potřebné licence pro řádné fungování a provoz částí díla a díla jako celku.
3. Zhotovitel výslovně prohlašuje, že je plně oprávněn disponovat právy k duševnímu vlastnictví, včetně práv autorských zahrnutých v předmětu díla, a zavazuje se za tímto účelem zajistit řádné a nerušené užívání díla objednatelem, včetně zajištění souhlasů držitelů autorských práv v souladu s autorským zákonem.
4. Územní rozsah a časový rozsah licencí je definován v Příloze č. 1 Technická specifikace,

kapitola 5.

5. Zhotovitel se zavazuje, že prováděním plnění dle této smlouvy nezasáhne neoprávněně do autorských práv třetí osoby. Odpovědnost za neoprávněný zásah do autorských i jiných práv třetích osob nese výlučně zhotovitel.
6. Zhotovitel je povinen objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že objednatel nemohl předmět díla užívat řádně a nerušeně. Jestliže se jakékoli prohlášení zhotovitele v tomto článku ukáže nepravdivým nebo zhotovitel poruší jiné povinnosti podle tohoto článku smlouvy, jde o podstatné porušení této smlouvy a zhotovitel uhradí ve prospěch objednatele smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení povinnosti. Zaplacením smluvní pokuty není nijak dotčeno ani omezeno právo objednatele na náhradu škody, kterou lze vymáhat vedle smluvní pokuty v plné výši. S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací díla dle této smlouvy je zhotovitel povinen vždy smluvně zajistit možnost volného nakládání s těmito právy objednatel.

XIII.

Práva z vadného plnění

1. Dílo má vady, jestliže jeho provedení neodpovídá požadavkům uvedeným v této smlouvě, příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se k provedení díla nebo pokud neumožňuje užívání, k němuž bylo určeno a zhotoveno.
2. Objednatel má právo z vadného plnění z vad, které má dílo při převzetí objednatel, byť se vada projeví až později. Objednatel má právo z vadného plnění také z vad vzniklých po převzetí díla objednatel, pokud je zhotovitel způsobil porušením své povinnosti. Projeví-li se vada v průběhu 6 měsíců od převzetí díla objednatel, má se zato, že dílo bylo vadné již při převzetí, neprokáže-li zhotovitel opak.
3. Vady díla dle odst. 2 tohoto článku budou zhotovitelem odstraněny bezplatně.
4. Pro nahlašování, uplatňování a odstraňování vad platí podmínky uvedené v příloze č. 2 této smlouvy.
5. Objednatel má právo na odstranění vady dodáním nové věci nebo opravou; je-li vadné plnění podstatným porušením smlouvy, má také právo od smlouvy odstoupit. Právo volby plnění má objednatel.
6. Provedenou opravu vady díla zhotovitel objednateli předá písemným protokolem.

XIV.

Odpovědnost za škodu

1. Zhotovitel je povinen uhradit objednateli škodu, která mu vznikla vadným plněním, a to v plné výši. Zhotovitel rovněž objednateli uhradí náklady vzniklé při uplatňování práv z vadného plnění.
2. Nebezpečí škody na předmětu plnění nese zhotovitel v plném rozsahu až do převzetí příslušné části plnění objednatel bez vad a nedodělků.
3. Zhotovitel prohlašuje, že po celou dobu plnění svého závazku z této smlouvy bude mít sjednáno pojištění odpovědnosti za škodu způsobenou třetím osobám vyplývající z dodávaného předmětu plnění s limitním plněním na jednu pojistnou událost minimálně 5

mil. Kč.

4. V případě, že při činnosti prováděné zhotovitelem dojde ke způsobení prokazatelné škody objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu odstavce 3 tohoto článku, bude zhotovitel povinen tyto škody uhradit z vlastních prostředků.
5. Zhotovitel je povinen předat objednateli při podpisu této smlouvy kopie pojistných smluv na požadované pojištění dle odst. 3 tohoto článku smlouvy včetně všech dodatků nebo certifikáty příslušných pojišťoven prokazující existenci pojištění po celou dobu plnění dle této smlouvy (dobu trvání pojištění, jeho rozsah, pojištěná rizika, pojistné částky, roční limity a sublimity plnění a výši spoluúčasti). Certifikát dle předchozí věty nesmí být starší 1 měsíce.

XV. Sankce

1. V případě porušení povinností smluvních stran uložených jim touto smlouvou se smluvní strany dohodly na následujících smluvních pokutách:
 - a) V případě prodlení zhotovitele s rozšířením licencí ve sjednané lhůtě dle čl. V odst. 2 písm. a) této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 0,05 % z ceny díla bez DPH za každý započatý den prodlení.
 - b) V případě nedodržení lhůty pro předání částí díla dle čl. V. odst. 2, písm. b) – l) této smlouvy je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 0,2 % z ceny díla bez DPH za každý započatý den prodlení.
 - c) V případě nedodržení zhotovitelem garantované dostupnosti stanovené v příloze č. 2 (odstavec definice SLA, kategorie „Vysoká“) této smlouvy se zhotovitel zavazuje objednateli uhradit smluvní pokutu ve výši 5.000,- Kč za každou započatou hodinu nedodržení garantované dostupnosti.
 - d) V případě nedodržení lhůty splatnosti faktury, kterou od zhotovitele převzal objednatel k úhradě, se objednatel zavazuje zhotoviteli uhradit úrok z prodlení ve výši stanovené občanskoprávními předpisy.
 - e) V případě porušení povinnosti zhotovitele oznámit objednateli dle čl. II odst. 2 této smlouvy veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky provádění díla (zejména neoznámí-li zhotovitel změnu identifikačních údajů) je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000,- Kč za každou jednotlivou změnu, jež objednateli neoznámil.
 - f) V případě, že se zhotovitel nezúčastní pravidelných kontrolních dní v sídle objednatele dle čl. IX odst. 3 této smlouvy bez dřívějšího souhlasu objednatele s absencí zhotovitele či nezúčastní-li se zhotovitel jednání týkajícího se předmětu smlouvy na základě pozvánky objednatele dle čl. IX odst. 4 této smlouvy bez dřívějšího písemného souhlasu objednatele s absencí zhotovitele, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000,- Kč za každý jednotlivý takto zmařený průběh kontrolního dne či jednoho každého jednání týkajícího se předmětu smlouvy na základě pozvánky.
 - g) V případě, že zhotovitel nepředá či nedoručí zápis o průběhu a závěrech jednání týkajícího se předmětu smlouvy na základě pozvánky objednatele dle čl. IX odst. 4 této smlouvy či kontrolního dne dle čl. IX odst. 5 této smlouvy objednateli ani do pěti pracovních dní ode dne konání jednání či kontrolního dne, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000,- Kč, a to za každý i započatý den prodlení s předáním či doručením každého takového zápisu.
 - h) V případě nepředá-li či nedoručí-li zhotovitel objednateli Zprávu o pokroku prací dle čl. IX

odst. 6 této smlouvy, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000,- Kč, a to za každý i započatý týden prodlení s předáním či doručením Zprávy o pokroku prací.

- i) V případě porušení povinnosti získat písemný souhlas objednatele se změnou poddodavatele dle čl. IX odst. 9 nebo nedodržení povinnosti obsadit pozici vedoucího nebo člena realizačního týmu osobou, splňující příslušné požadavky dle zadávací dokumentace na veřejnou zakázku, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000,- Kč za každý započatý den nedodržení povinnosti.
 - j) V případě porušení povinnosti dle čl. XIV odst. 3 této smlouvy, tj. povinnosti mít po celou dobu platnosti této smlouvy sjednanou pojistnou smlouvu pro případ způsobení škody třetí osobě s limitním plněním na jednu škodnou událost minimálně 5 mil. Kč, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 10.000 Kč za každý i započatý měsíc, v němž nebude mít uzavřenou pojistnou smlouvu se stanovenými parametry.
 - k) Nevystaví-li a současně nedoručí-li zhotovitel fakturu objednateli dle podmínek této smlouvy k části díla, kterou již objednatel řádně převzal a převzetí stvrdil v předávacím protokolu, ani do 5 pracovních dní od výzvy objednatele k vystavení faktury zhotovitelem, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 1.000,- Kč za každý započatý den prodlení s vystavením a doručením faktury.
2. Smluvní pokuta a úrok z prodlení jsou splatné do 30 dní ode dne doručení písemného vyúčtování příslušné výše povinné straně.
 3. Zaplacením jakékoli smluvní pokuty není dotčen nárok objednatele na náhradu škody, objednatel má nárok na náhradu škody vedle smluvní pokuty v plné výši. Zaplacením smluvní pokuty není dotčena povinnost splnění povinnosti, která je prostřednictvím smluvní pokuty zajištěna.

* XVI. Zánik smlouvy

1. Smluvní strany se dohodly, že smlouva zaniká:
 - a) Dohodou smluvních stran,
 - b) Jednostranným odstoupením od smlouvy pro její podstatné porušení druhou smluvní stranou, přičemž podstatným porušením smlouvy se rozumí zejména:
 - neprovedení díla (jeho části) v termínech plnění dle čl. V odst. 2. této smlouvy,
 - nedodržení pokynů objednatele, právních předpisů nebo technických norem, které se týkají provádění díla,
 - nedodržení smluvních ujednání o záruce za jakost nebo o právech z vadného plnění,
 - neuhrazení ceny za dílo objednatelem po druhé výzvě zhotovitele k uhrazení dlužné částky, přičemž druhá výzva nesmí následovat dříve než 30 dnů po doručení první výzvy.
2. Objednatel je dále oprávněn od této smlouvy odstoupit v těchto případech:
 - bylo-li příslušným soudem rozhodnuto o tom, že zhotovitel je v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení

(insolvenční zákon), ve znění pozdějších předpisů (a to bez ohledu na právní moc tohoto rozhodnutí);

- podá-li zhotovitel sám na sebe insolvenční návrh.

3. Pro účely této smlouvy se pod pojmem „bez zbytečného odkladu“ dle § 2002 občanského zákoníku rozumí „nejpozději do 3 týdnů“.

XVII. Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem, kdy vyjádření souhlasu s obsahem návrhu smlouvy dojde druhé smluvní straně, pokud nestanoví zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), jinak. V takovém případě smlouva nabývá platnosti dnem jejího podpisu smluvními stranami a účinnosti uveřejněním v registru smluv. Objednatel neprodleně oznámí zhotoviteli informaci o zveřejnění smlouvy v registru smluv.
2. Doplnění nebo změnu této smlouvy lze provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, vzestupně číslovaných a takto označených dodatků.
3. Zhotovitel nemůže bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí z této smlouvy třetí straně.
4. Tato smlouva je vyhotovena v 6 stejnopisech s platností originálu, přičemž objednatel obdrží 5 a zhotovitel 1 její vyhotovení.
5. Zhotovitel bere na vědomí a výslovně souhlasí s tím, že smlouva včetně příloh a případných dodatků bude zveřejněna na oficiálních webových stránkách Moravskoslezského kraje. Je-li zhotovitel fyzickou osobou, bude smlouva zveřejněna po anonymizaci provedené v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
6. Smluvní strany se dohodly, že pokud se na tuto smlouvu vztahuje povinnost uveřejnění v registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), provede uveřejnění v souladu se zákonem objednatel.
7. Nedílnou součástí této smlouvy jsou následující přílohy:
 - Příloha č. 1 – Technická specifikace*
 - Příloha č. 2 – Technická podpora IDM MSK*
 - Příloha č. 3 – Cena*
 - Příloha č. 4 – Podrobný položkový rozpis všech nutných licencí SW*
 - Příloha č. 5 – Seznam poddodavatelů zhotovitele*
8. Doložka platnosti právního jednání dle § 23 zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů: K uzavření této smlouvy má objednatel souhlas rady kraje udělený usnesením č. 25/2167 ze dne 21. 11. 2017

V Ostravě dne: 28 .12. 2017

V Praze dne: 28 .12. 2017



za objednatele

prof. Ing. Ivo Vondrák, CSc.
hejtman kraje



za zhotovitele

Ing. Martin Řehořek

Po dobu nepřítomnosti zastoupen
Jiřím Navrátillem
náměstkem hejtmána kraje

NEWPS.CZ s.r.o. ³
Přemyslovská 2845/43, 130 00 Praha 3
IČ: 25625632, DIČ: CZ25625632



Příloha č. 1 - Technická specifikace

1. Popis současného stavu

Moravskoslezský kraj v současné době využívá systém pro správu identit, který byl pořízen v rámci projektu e-Government Moravskoslezského kraje (II. – VI. část výzvy) spolufinancovaného z Integrovaného operačního programu. Dodavatelem systému je společnost NEWPS.CZ s.r.o., v rámci projektu byla uzavřena Smlouva o poskytování služeb vnitřní integrace úřadu, poskytnutí licencí a zajištění dalších souvisejících služeb.

Kraj disponuje licencí pro 750 interních identit zařazených do Krajského úřadu a 4530 licencí pro identity externích organizací. Systém je intenzivně rutinně využíván jak v rámci interní sítě Krajského úřadu, tak v rámci poskytování sdílených služeb zřizovaným organizacím. Přes autentizační brány prochází denně tisíce přístupů k aplikacím. Například denní průměr za měsíc únor 2017 byl 18 tisíc webových stránek v rámci 3 tisíc návštěv uživatelů.

Systém využívá jako primární zdroj identit zaměstnanců kraje personální systém Krajského úřadu Moravskoslezského kraje. Identity z orgánů veřejné moci (obce kraje) čerpá z Jednotného identitního prostoru na který je napojen. A identity zařazené do zřizovaných a dalších externích organizací jsou zadávány prostřednictvím portálu uživatele ručně lokálními správci z řad příslušných organizací.

Interní identity jsou systémem propagovány do Active Directory a zároveň je interním identitám zřizována e-mailová schránka v MS Exchange serveru. Systém disponuje dvěma autentizačními branami pro aplikace s webovým rozhraním. Interní pro uživatele přistupující z ICT prostředí Krajského úřadu a externí pro uživatele přistupující z prostředí internetu. Interní brána je napojena na Active Directory doménu krajského úřadu pro zajištění jednotného přihlášení uživatelů (uživatel se hlásí pouze do operačního systému, odkud je autentifikace převzata).

Se systémem pro správu identit jsou integrovány především aplikace s webovým rozhraním a to na různých stupních integrace. Do některých aplikací systém aktivně propaguje zakládané identity včetně autorizačních údajů, jiné si údaje o uživateli a jejich oprávněních přebírají samy v pravidelných intervalech nebo v okamžiku přístupu uživatele do aplikace, další pouze přebírají identitní informace uživatele bez řízení oprávnění na úrovni systému pro správu identit.

Systém se aktuálně nachází ve fázi udržitelnosti projektu a to do 31. 5. 2020. Vzhledem ke skutečnosti, že držitelem autorských práv na dodaný systém správy identit je společnost NEWPS.CZ s.r.o, a že systém je nutné v rámci období udržitelnosti zachovat, je jediný možný dodavatel rozšíření a úprav tohoto systému společnost NEWPS.CZ s.r.o.

Tyto skutečnosti také dokladuje prohlášení společnosti NEWPS.CZ s.r.o:

NEWPS.CZ

Member of WFS Group

NEWPS.CZ s.r.o.

Sídlem: Přemyslovská 2845/43, 130 00 Praha 3

IČ: 25625632

DIČ: CZ25625632

Zapsaná: u Městského obch. Soudu v Praze, odd. C, vložka č. 55889

Zastoupená: Ing. Martinem Řehořkem, jednatelem


Prohlašuje:

Softwarové komponenty řešení systému pro správu identit realizovaného na základě projektu „e-Government Moravskoslezského kraje (II. – VI. část výzvy)“ jsou vlastnictvím společnosti NEWPS.CZ s.r.o.

Současně je společnost NEWPS.CZ s.r.o. výhradním správcem autorských práv k tomuto dílu. Součástí dodávky díla nebylo garantované veřejné rozhraní umožňující integraci třetími stranami. Současně upozorňujeme, že případné neoprávněné zásahy do systému mohou vést k odmítnutí plnění technické podpory svázané s tímto projektem.

V Praze dne 13.6.2016

.....
Ing. M. Řehořek
jedenatel

NEWPS.CZ s.r.o. 
Přemyslovská 2845/43, 130 00 Praha 3
IČ: 25625632, DIČ: CZ25625632

Prohlášení

My,

NEWPS.CZ s.r.o.

Sídelní: Přemyslovská 2845/43, 130 00 Praha 3

IČO: 25625632

DIČ: CZ25625632

Zapsaný: u Městského obch. soudu v Praze, oddíl C., vložka číslo 55889

Zastoupený: Ing. Martinem Řehořkem, jednatelem

prohlašujeme, že

software PUMA IAM Advanced Edition byl krajskému úřadu Moravskoslezského kraje dodán dle podmínek zadávací dokumentace veřejné zakázky „Vnitřní integrace úřadu“, jako ucelené řešení, ke kterému zhotovitel poskytl nevýhradní oprávnění k užití v souladu se smlouvou. Z důvodu technické architektury a celkové koncepce navrženého, dodaného akceptovaného řešení nelze stávající licenci rozšířit tak, aby byl zadavatel oprávněn k zásahům do systému v rozsahu předmětu studie proveditelnosti.

Licenční práva na tento produkt a s ním spojené know-how jsou ve výhradním vlastnictví společnosti NEWPS.CZ s. r. o.

Za

NEWPS.CZ s.r.o.

Ing. Martinem Řehořkem, jednatelem

NEWPS.CZ s.r.o.
Přemyslovská 2845/43, 130 00 Praha 3
IČ: 25625632, DIČ: CZ25625632

2. Důvody rozšíření a rozvoje stávajícího systému správy identit

Současný stav systému pro správu identit byl dimenzován v roce 2012. Přestože se přihlíželo k dalšímu vývoji požadavků a systém se dimenzoval s kapacitní a funkční rezervou, ukázala se tato rezerva jako velmi nedostačující. V současné době se velmi intenzivně rozšiřují sdílené služby poskytované zřizovaným organizacím z technologického centra kraje, jsou nové požadavky na rozvoj aplikační podpory komunikace a spolupráce s obcemi kraje a také se mění standard práce na projektech, kdy je v rámci společné práce na dokumentech nebo v aplikacích potřeba zapojovat uživatele z externích společností. Na systém jsou také kladeny také požadavky z důvodu rozvoje legislativního prostředí České republiky a Evropské unie. Díky tomuto rozvoji požadavků je potřeba rozšířit jak kapacitu, tak funkcionalitu systému pro správu identit Moravskoslezského kraje.

Mimo dalších informačních systémů Moravskoslezský kraj plánuje a připravuje zavedení dvou stěžejních systémů: jednotného sdíleného personálního systému a jednotného sdíleného ekonomického systému pro zřizované organizace. Zprovoznění těchto systémů s sebou nese požadavek na zapojení všech zaměstnanců krajem zřizovaných a zakládaných organizací do Systému pro správu identit. Zároveň z analýz proveditelnosti těchto systémů vychází, že v současné době není

Správa identit krajské korporace | Tento projekt je spolufinancován z prostředků Evropské unie

reálné tyto systémy poskytovat s webovým rozhraním a bude potřeba připravit infrastrukturu pro poskytování sdílených aplikačních služeb s těžkými klienty, do které bude přístupy řídit systém pro správu identit. Výrazným benefitem realizace jednotného personálního systému je možnost napojit na něj správu identit jako na zdroj identit zřizovaných organizací.

V návaznosti na jednotný personální systém velké zřizované organizace uvažují o provozování vlastních systémů pro správu identit, které by zabezpečovaly autentizaci a autorizaci systémů provozovaných těmito organizacemi. Proto by bylo potřeba mít možnost napojení lokálních systémů pro správu identit na systém provozovaný krajem.

Z hlediska rozvoje legislativy jsou nové požadavky na funkcionalitu systému pro správu identit kladeny především nařízením eIDAS o elektronické identifikaci a službách vytvářejících důvěru, které přináší především možnost zapojit se do standardizovaných evropských struktur pro sdílení identit. A zákon o kybernetické bezpečnosti, který klade nové podmínky na provozování významných informačních systémů, do kterých mnoho krajem provozovaných systémů spadá.

3. Popis cílového stavu

Systém pro správu identit bude provozován v technologickém centru MSK. Pro komponenty systému bude vytvořena demilitarizovaná zóna. Všechny systémy a služby budou napojeny na centrální dohled a management kraje.

Základní komponentou centralizovaného systému pro správu identit je vysoce dostupná databáze identit (e-directory) poskytující přístup k informacím o identitách protokolem LDAP. Informační model LDAP (schéma) bude založen na standardech. Přístup do e-directory budou mít pouze vnitřní komponenty řešení IDM. Externí systémy (personální systémy, jiné IDM systémy, integrované aplikace) budou pracovat s obsahem e-directory nepřímo pouze prostřednictvím definovaných rozhraní, která bude poskytovat řešení IDM (např. rozhraní webových služeb).

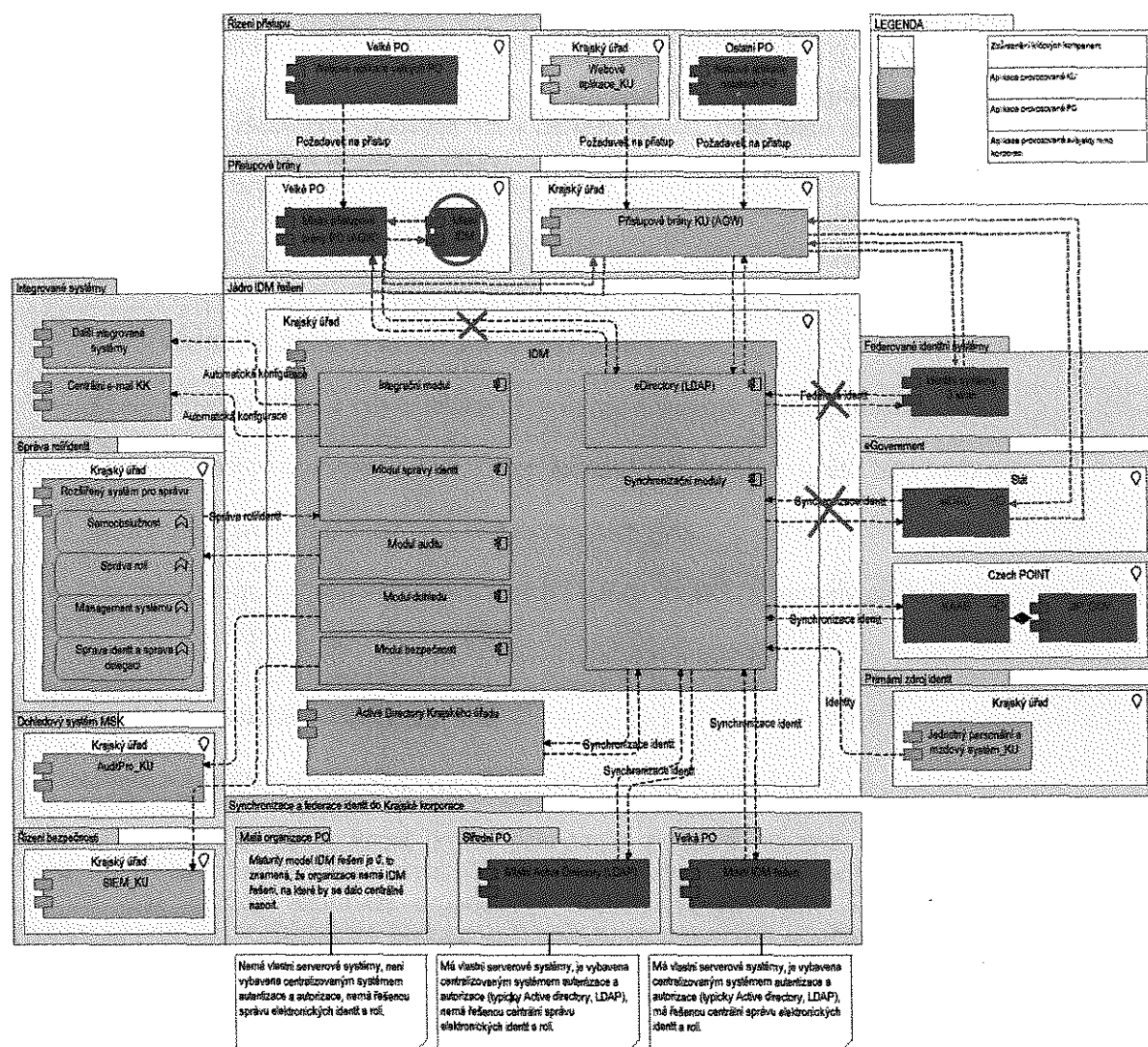
Modifikace obsahu e-directory bude primárně zajištěna automatizovaně synchronizačními moduly a dále bude povolena manuální modifikace z aplikace pro správu. Změnit bude možné jen modifikovatelné atributy; nebude možné měnit aplikační, systémové a atributy, které jsou předmětem synchronizace dat. Prováděné operace budou zaznamenány do auditního logu. Zhotovitel specifikuje datové zdroje a cíle pro synchronizaci, časovou linii synchronizace a napojená workflow. Zhotovitel vytvoří/rozšíří aplikaci pro správu identit tak aby umožňovala efektivní správu všech rolí a identit.

Všechny operace realizované integračními moduly budou zaznamenány do auditního logu.

Systémově lze jednotlivé moduly implementovat jako samostatné procesy na různých serverech. Preferované je řešení nevyžadující komerční licence. Všechny moduly musí být napojeny na centrální dohled a SIEM.

Součástí řešení jsou vysoce dostupné autentizační (v omezené míře rovněž autorizační) brány implementující SSO. Primárním zdrojem identit pro SSO je e-directory.

Komplexní schéma řešení cílového stavu IDM:



4. Analýza a prováděcí návrh úprav a rozvoje systému správy identit

Jedná se o jeden dokument, který bude vycházet z aktuálního stavu implementace systému pro správu identit v ICT prostředí Moravskoslezského kraje, a který bude podrobně popisovat detaily implementace jednotlivých částí předmětu této smlouvy - článek III odst. 2.1 písm. c) až l) této smlouvy.

Dokument Analýzy bude zpracován v souladu s Manuálem jednotného vizuálního stylu Moravskoslezského kraje, který je dostupný na webu kraje. Každá jednotlivá strana Analýzy bude v záhlaví či v zápatí označena prvky povinné publicity, názvem projektu, registračním číslem projektu. Dokument bude zpracován podle zásad a v souladu s ČSN 01 6910 „Úprava písemností zpracovaných textovými editory“ v aktuálním platném znění. Dokument bude zpracován v souladu a rozsahu s popsanou detailní specifikací zadavatele, která je součástí této smlouvy.

Veškeré obrázky využitě v Analýze budou ve formátu JPG nebo GIF (u obrázků s rozlišením do 256 barev). Na titulní stránce Analýzy bude uvedeno: název dokumentu, název projektu, registrační číslo projektu, číslo veřejné zakázky, číslo smlouvy, označení zhotovitele označení objednatele, prvky publicity.

Zhotovitel prohlašuje, že při tvorbě Analýzy bude dbát autorských práv třetích stran.

Při zpracování Analýzy se zhotovitel zavazuje konzultovat svůj postup s objednatelem. Analýza bude

podrobená oponentuře objednatelem nebo jím vybraným oponentem. S tímto je nutné počítat v harmonogramu tvorby Analýzy a min. posledních 14 dní před odevzdáním této části díla umožnit objednateli oponenturu provést a zapracovat jeho případné připomínky.

Analýza bude předána ve třech vyhotoveních na přenosném mediu v digitální podobě (formát doc, xls a PDF), a to včetně všech podkladových dat v českém jazyce. Dále bude Analýza předána vytištěná ve třech vyhotoveních svázaná do pevné vazby.

Obsahem dokumentu minimálně bude:

- Manažerský souhrn,
- Popis výchozího stavu systému pro správu identit kraje,
- Popis cílového stavu a návrh nezbytných úprav a rozvoje systému správy identit,
- Analýza a návrh postupu implementace jednotlivých částí předmětu této smlouvy,
- Souhrnná analýza technických a bezpečnostních rizik,
- Harmonogram postupu implementačních částí (v souladu s termíny plnění).

5. Minimální technické požadavky

Rozšíření stávajících licencí na geografickou multilicenci, počet licencí

Současný stav k 1. 5. 2017: Počet licencí pokrývající aktuálně plánované systémy se pohybuje na úrovni 40 tisíc uživatelů (20 tisíc uživatelů kraje a jím zřízené organizace, 15 tisíc uživatelé obcí a 5 tisíc uživatelé dalších externích organizací). Z ekonomických důvodů – multilicenční sleva a předpokladu dalšího rozšiřování v budoucnosti požadujeme **povýšit současnou licenci systému** pro správu identit na:

- **časově neomezenou multilicenci** pro neomezený počet uživatelů geograficky vázaných na Moravskoslezský kraj a jeho území (vázaností se rozumí to, že uživatel musí při využívání IDM MSK být v zaměstnaneckém, služebním či obdobném vztahu k Moravskoslezskému kraji (dále také „geografická multilicence“),
- a **1000 doplňkových časově neomezených licencí** pro uživatele externích organizací mimo Moravskoslezský kraj.

Úprava portálu samoobslužného řešení

Zhotovitel navrhne a provede úpravy portálu uživatele směrem ke zvýšení uživatelské přehlednosti při práci s více rolemi, organizacemi, uživateli a doplnění nových funkcionalit. Úpravy budou minimálně obsahovat:

- umožnění manuálního zakládání uživatelů v rámci organizací, které mají jako zdroj identit personální systémy (včetně Krajského úřadu) s možností manuálního přiřazování business a aplikačních rolí (možnost zadání uživatele bez zaměstnaneckého vztahu – externí účetní, auditor, a podobně),
- možnost uživatele požádat o přidělení oprávnění, žádost bude podléhat schválení podle parametrizovaného workflow,
- možnost parametricky řídit maximální počet přidělení rolí za jednotlivou roli, všech rolí za

aplikační informační systém a maximální počet přidělení role v rámci organizace – z důvodu dodržování licenčních politik integrovaných informačních systémů, pokud by měl být maximální počet přidělení role překročen, systém pro správu identit přidělení role odmítne,

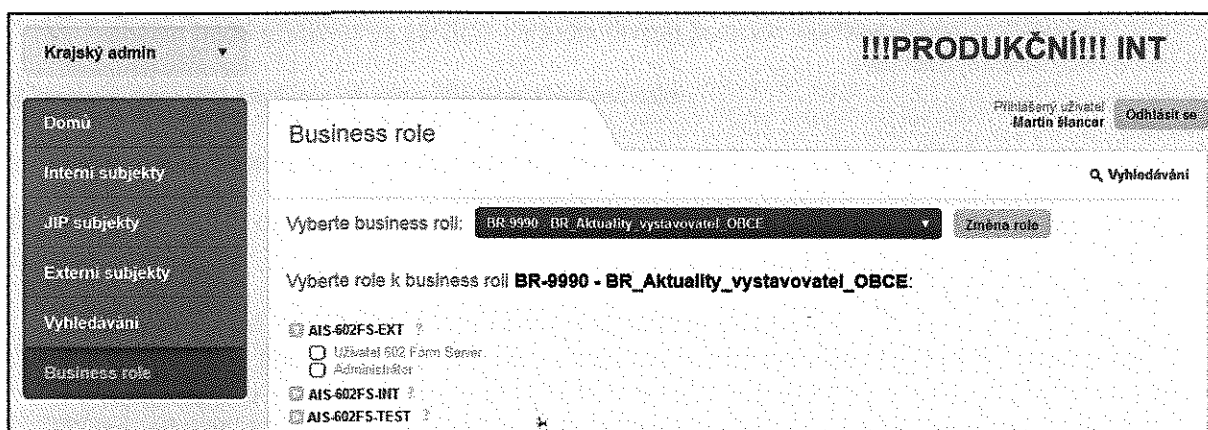
- zafixování levých sloupců a hlaviček sloupců ve formulářích, kde se zpracovává větší počet řádků a sloupců, v současném stavu je konfigurace velmi nepřehledná a vede k chybám,
- zvýšení uživatelské přívětivosti rozhraní portálu.

Závazná detailní technická specifikace zhotovitele

Úprava portálu samoobslužného řešení bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem.

Samoobslužný portál bude upraven za účelem zlepšení celkového uživatelského komfortu a přívětivosti a to následně. Budou upraveny stránky, kde se zobrazuje větší množství údajů – stránka pro správu rolí, organizací, uživatelů.

Stránka pro definici business rolí bude upravena tak, že aplikační role budou sdruženy podle jednotlivých AISů – viz ilustrativní obrázek:



Nebudou tedy najednou zobrazovány všechny aplikační role.

Bude zvýšena rychlost zobrazování přehledu uživatelů a do filtru uživatelů budou přidány další možnosti filtrování podle:

- příznaku zablokování účtu
- blokování přístupu

Další rozšíření portálu budou zahrnovat:

- Možnost založit ručně uživatele u organizací s automatickým zakládáním identit z HR systému.
- Možnost založit uživatele bez zaměstnanecké pozice.
- Možnost ručně přidělit business a aplikační roli uživateli.
- Možnost řídit parametricky maximální počet přidělovaných rolí ve vazbě:
 - na konkrétní roli – danou roli lze přiřadit jen N-krát
 - na konkrétní AIS – v rámci daného AIS lze přiřadit celkově jen N rolí
 - na konkrétní subjekt – v rámci daného subjektu lze uživatelům přiřadit celkově jen N rolí
- Zafixování levých sloupců a hlaviček sloupců ve formulářích, kde se zpracovává větší počet řádků a sloupců.

Bude umožněna blokace rolí a činnostních rolí.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo navýšení původního stavu, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí (například pro operační systém), pokud to tato funkcionality bude vyžadovat.

Rozšíření IDM o workflow modul

Zhotovitel navrhne a implementuje workflow modul pro zpracování požadavků na přidělení rolí. Modul bude umožňovat:

- řídit průběh schvalování přidělení role uživateli,
- průběh schvalování bude možné parametricky měnit,
- o změně stavu tiketů budou dotčení uživatelé informováni e-mailem (avizační e-mailové zprávy),
- uživatelé na pozicích ve workflow budou definováni konkrétní identitou, rolí, organizační strukturou (nadřazený),
- systém bude pracovat se zástupy na jednotlivých pozicích workflow.

Závazná detailní technická specifikace zhotovitele

Workflow modul bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem.

Řešení IDM bude rozšířeno o samostatný workflow modul, který bude obsahovat následující funkcionality:

- Uživatel bude moci požádat o přidělení role nebo skupiny rolí.
- Schvalovatel bude moci schválit nebo zamítnout žádost o přidělení role nebo skupiny rolí.
- Administrátor bude moci definovat průběh schvalovacích workflow v podobě BPMN diagramu.
- Na základě definovaného workflow bude možné účastníkům workflow zasílat e-mailové notifikace.
- Role bude možné sdružovat do skupin rolí pro zefektivnění žádání o více souvisejících rolí najednou.
- Žadatel nevybírá, které schvalovací workflow se má spustit. Místo toho se automaticky spouští to workflow, které je přiřazeno k dané roli.

Schvalování přiřazení role bude probíhat následovně:

1. Žadatel se přihlásí do Workflow modulu.
2. Žadatel založí novou žádost o přiřazení role. V žádosti zadá pomocí vyhledávače roli, o kterou žádá.
3. Systém načte workflow, které je svázáno s danou rolí, a začne je vykonávat.
4. V rámci workflow mohou probíhat tyto aktivity (nastávat události): na účastníka je odeslána e-mailová notifikace, schvalovatel schválí žádost, schvalovatel zamítne žádost, dojde k „timeoutu“ žádosti (schvalovatel se nestihne vyjádřit včas).

Workflow je tedy prováděno sekvenčně podle definovaného BPMN diagramu a v případě učiněného rozhodnutí (schválení, zamítnutí, „timeout“) se pokračuje příslušnou větví k další aktivitě. Na konci workflow je žádost o přidělení role schválena, zamítnuta, nebo nebyla vyřízena v definované časové lhůtě.

Schvalovací proces bude parametricky definován pomocí zjednodušeného BPMN diagramu. Workflow

bude moci editovat administrátor v případě, že není spuštěno žádné schvalovací workflow podle dotyčného BPMN diagramu.

Administrátor bude dále definovat skupiny rolí. Bude možné vytvářet hierarchický strom, tj. skupina rolí může v sobě obsahovat další skupinu rolí.

Jednotlivé účastníky workflow bude možné identifikovat podle uživatelského jména, organizačního zařazení, nebo podle role. Pokud nebude některá identifikace osoby jednoznačná (např. určitou roli bude mít více osob), pak bude žádost postoupena na všechny tyto osoby a postačí, když ji schválí pouze jediná osoba.

Po přihlášení do modulu Workflow se všem uživatelům zobrazí tzv. dashboard, na kterém se jim zobrazí stav jimi podaných žádostí o přidělení role a také seznam žádostí čekajících na schválení, pokud patří mezi schvalující osoby.

Modul Workflow bude řešit zastupování definováním dalších schvalovatelů ve workflow. Zástupce může být vyzván ke schválení žádosti, pokud se hlavní schvalovatel nevyjádří např. do 48 hodin, nebo může být žádost zaslána na hlavního schvalovatele i zástupce zároveň a bude schválena, když ji alespoň jeden z nich schválí.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo navýšení původního stavu, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí (například pro operační systém), pokud to tato funkcionality bude vyžadovat.

System zasilání logů do SIEM

Zhotovitel ve spolupráci s objednatelem navrhne způsob a napojí systém pro správu identit na SIEM auditních logů. Nástroj SIEM je řešen samostatně v rámci plnění veřejné zakázky „Pořízení nástroje SIEM včetně funkcionality pro audit logů“. Součástí dodávky zhotovitele bude:

- napojení na SIEM.

Závazná detailní technická specifikace zhotovitele

IDM bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem.

Pro potřeby nástroje SIEM bude realizovaná funkcionality, která bude do samostatného logu zaznamenávat tyto události o hlavních objektech Subjekt, Role, Uživatel a AIS:

- Vytvoření hlavních objektů
- Změna hlavních objektů
- Smazání/zablokování hlavních objektů
- Synchronizace objektů

Tato funkcionality bude implementována v rámci všech komponent systému.

Předpokládáme, že takto vytvářený log v řešení IDM bude nástroj SIEM schopen číst vlastními prostředky a sondami z určeného prostředí.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo navýšení původního stavu, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí (například pro operační systém), pokud to tato funkcionality bude vyžadovat.

Typová instalace a konfigurace otevřeného vzorového konektoru (vzor pro HR systémy)

Zhotovitel ve spolupráci s objednatelem navrhne a naimplementuje typové rozhraní pro synchronizaci identit z personálních systémů do systému pro správu identit a propagaci identit ze systému pro správu identit. Parametry dodané řešení:

- řešení integrace personálních systémů bude postaveno na webových službách,
- parametricky bude definovatelné ověření personálního systému, který webovou službu volá (například tokenem),
- podrobná specifikace a dokumentace webových služeb včetně doporučeného postupu integrace personálního systému a otestování,

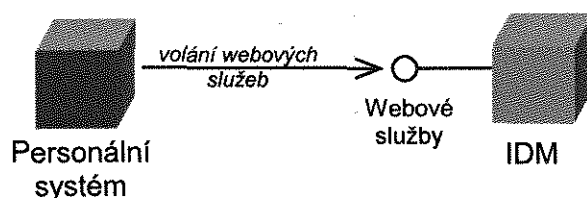
Závazná detailní technická specifikace zhotovitele

Integrace řešení IDM s HR systémem a vytvoření vzorového konektoru pro integraci s IDM systémy bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem

HR systémy integrované s řešením IDM musí dále správně pracovat s tzv. plánovanými činnostmi a aktivitami identit. Tato problematika je podrobněji popsána níže a je v režii samotné organizace, případně MSK.

Synchronizace identit z HR systému do systému IDM

Synchronizace identit mezi HR systémem a řešením IDM bude založena na používání webových služeb. Personální systém bude vystupovat v roli autoritativního zdroje dat, který volá webové služby za účelem propagace nových identit a změn ve stávajících identitách do řešení IDM.



Webové služby budou synchronní služby založené na standardu REST a budou personálním systémům poskytovat tyto funkcionality:

- Vytvoření identity
- Změna identity – zahrnuje rovněž zablokování a odblokování účtu

V rámci implementace bude dodána podrobná specifikace a dokumentace webových služeb. Webové služby budou pracovat s těmito údaji uživatele:

- Jednoznačný identifikátor identity napříč IDM (GUID)
- Uživatelské jméno
- Titul před
- Jméno
- Příjmení
- Titul za
- Fotografie
- Sekce (včetně příslušných vazeb)
- Odbor (včetně příslušných vazeb)
- Oddělení (včetně příslušných vazeb)
- Kancelář
- Budova

- Funkce
- Nadřazený
- Adresa
- E-mailová adresa
- Telefonní číslo
- URL adresa
- Pohlaví
- Datum narození
- Místo narození
- Rodné číslo
- Platné doklady
- Číslo občanského průkazu
- Číslo pasu
- Seznam zastávaných business rolí
- Příznak aktivity identity
- Aktivní od
- Aktivní do

Parametrické ověření HR systémů přistupujících k webovým službám

Komunikace HR systému s webovými službami bude zabezpečena pomocí klientského SSL/TLS.

HR systém bude do IDM zaregistrován jako speciální AIS a vůči webovým službám se bude autentizovat certifikátem, uloženým v nastavení AIS. Musí se jednat o komerční serverový certifikát vystavený českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Speciální požadavky na personální systémy

Personální systémy musí správně přistupovat k problematice tzv. plánovaných akcí a k určování tzv. aktivity identity uživatele.

Tzv. plánovaná akce je činnost, kterou pracovník HR zadá do personálního systému v čase T_1 , ale k této činnosti má dojít např. v čase $T_2 = T_1 \pm 10$ dní. Personální systém musí tuto činnost propagovat do IDM až v čase T_2 , kdy k dané události dojde; ne v čase T_1 , kdy je tato budoucí událost pouze zaznamenána k vykonání.

Pokud by např. danou plánovanou činností bylo ukončení pracovního poměru, mohlo by při nesprávném ošetření plánovaných činností personálním systémem dojít k tomu, že účet uživatele bude zablokován několik dní či týdnů před skutečným ukončením pracovního poměru a tím mu bude znemožněno vykonávat svoji práci.

Aktivita identity se typicky určuje na základě příznaku neaktivity v personálním systému (je-li v něm taková funkce implementována) a na základě počtu evidovaných pracovních poměrů, jejich aktivity a dalších položek jako jsou mimo evidenční stavy a podobně.

Jakákoliv změna těchto skutečností musí vést k zapsání informace o zablokování či odblokování identity do IDM a je nutným předpokladem pro integraci personálního systému.

Specifikace integračního rozhraní pro integraci aplikací

Zhotovitel navrhne a naimplementuje rozhraní pro synchronizaci identit, údajů vedených o identitách a přidělených oprávnění ze systému pro správu identit do integrovaných aplikačních systémů. Dodané řešení bude obsahovat:

- webové služby, voláním kterých budou integrované aplikace data získávat,

- parametricky bude definovatelné ověření aplikace, která webovou službu volá (například tokenem),
- dostupný podrobný popis rozhraní synchronizačního konektoru a doporučený postup implementace.

Závazná detailní technická specifikace zhotovitele

Návrh a implementace integračního rozhraní pro integraci jiných aplikací bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem

Definice webových služeb pro integraci jiných aplikací s IDM

Integrace jiných aplikací s IDM bude založena na volání webových služeb IDM těmito jinými aplikacemi. Řešení IDM bude pro jiné aplikace publikovat webové služby založené na standardu REST, které budou poskytovat tyto funkcionality:

- Stažení seznamu uživatelů
- Stažení detailu uživatelského účtu

Technická specifikace těchto webových služeb bude definována během implementační fáze.

Komunikaci s webovými službami budou iniciovat jiné aplikace, které zašlou požadavek na vrácení seznamu uživatelů. Následně z odpovědi webové služby vyhodnotí, u jakých účtů došlo ke změně, a požádají o poskytnutí detailních informací o těchto účtech. Identifikované změny si uloží do své databáze.

Jiné aplikace nebudou mít právo zpětně do IDM zapisovat údaje o uživateli.

Tímto způsobem nebude možné synchronizovat hesla ani jiné přihlašovací údaje uživatelů. Tyto jiné aplikace by měly být integrovány s přístupovými bránami AGW a důvěřovat jimi provedené autentizaci uživatelů, čímž se jakákoliv potřeba synchronizace přihlašovacích údajů eliminuje.

Ověření přístupujících aplikací k webovým službám

Komunikace jiných aplikací s webovými službami bude zabezpečena pomocí SSL/TLS.

Jiná aplikace bude do IDM zaregistrována jako AIS a vůči webovým službám se bude autentizovat certifikátem, uloženým v nastavení AIS. Musí se jednat o komerční serverový certifikát vystavený českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Úprava systému rolí, propagace rolí (implementace RBAC)

Zhotovitel navrhne a vyvine rozšíření správy business a aplikačních rolí, které umožní:

- využívat funkcionalitu business rolí u všech typů uživatelů systému pro správu identit (v současné době možné jen u uživatelů z Krajského úřadu),
- propagovat business a aplikační role z integrovaných aplikací nebo jiných informačních systémů do systému pro správu identit za pomoci webových služeb,
- přiřazovat business a aplikační role uživatelům za pomoci volání webových služeb,
- propagovat uživatele do integrovaných Active Directory případně dalších integrovaných IDM systémů podle rolí přiřazených uživatelům, které slouží pro přístup do informačních systémů. Propagaci uživatelů bude možné parametricky řídit definováním konkrétních rolí, které musí

mít propagovaní uživatelé přiřazeny, nebo definováním konkrétních informačních systémů, kdy propagovaný uživatel musí mít přiřazenu libovolnou roli používanou v daném systému,

- propagovat role přiřazené uživatelům ze systému pro správu identit do napojených Active Directory za účelem řízení oprávnění uživatelů v aplikacích s těžkým klientem napojených na Active Directory. Parametricky bude možné definovat, které role se budou propagovat do kterých Active Directory.

Dodávka bude obsahovat podrobnou dokumentaci volání vyvinutých webových služeb.

Závazná detailní technická specifikace zhotovitele

Úprava systému rolí bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem.

Rozšíření funkcionality business rolí na všechny uživatele

Řešení IDM bude rozšířeno tak, aby umožňovalo nastavovat business role všem uživatelům v systému. Pro rozklad business rolí na aplikační role bude použit stejný mechanismus, který je používán v současném řešení IDM.

Webové služby pro import aplikačních rolí

Pro integrované aplikace bude vytvořena nová webová služba, která bude přijímat základní informace ohledně definice rolí obsažených v integrované aplikaci. Tato webová služba bude umožňovat přidávání nových aplikačních rolí, které vznikly například v průběhu implementace integrované aplikace. Tato funkcionality je určena jednak pro integrátory aplikací, aby správu rolí bylo možné provádět i jinak než ručním způsobem, jednak ji bude možné využít v situacích, kdy ve vyvíjené aplikaci vnikne nová role.

Tato webová služba bude synchronní a bude založena na standardu REST. Přístup k této službě budou mít jen integrované aplikace zaregistrované v řešení IDM jako lokální AIS.

Webové služby pro přidělování business rolí

Bude vytvořena webová služba, která bude umožňovat vytváření business rolí v IDM v rámci daného AIS (integrované aplikace) a k nim náležících aplikačních rolí. Tedy daný AIS bude moci specifikovat jenom role, které sám definuje.

Tato webová služba bude synchronní a bude založena na standardu REST. Přístup k této službě budou mít jen integrované aplikace zaregistrované v řešení IDM jako lokální AIS.

Parametrická propagace uživatelů a rolí

Administrátor bude moci řídit propagaci uživatelů do integrovaných Active Directory a dalších IDM systémů na základě rolí přidělených uživatelům. Uživatel se do cílového systému bude propagovat jen tehdy, pokud bude mít přiřazenu aplikační roli odpovídající filtračním pravidlům.

Administrátor bude moci dále řídit propagaci rolí do integrovaných Active Directory. Na základě definovaných podmínek bude moci určovat, do jaké Active Directory se запиše jaká role přidělená uživatelům. Role budou propagovány do Active Directory pouze jako identifikátory s jejich názvem.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo navýšení původního stavu, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí (například pro operační systém), pokud to tato funkcionality bude vyžadovat.

Škálování AGW pro vyšší výkon a dostupnost

Zhotovitel ve spolupráci s objednatelem navrhne a nasadí úpravy AGW bran pro zajištění vysoké dostupnosti a možnosti škálování. Systém minimálně umožní balancovat zátěž mezi AGW branami a přebírání provozu v případě výpadku brány.

Závazná detailní technická specifikace zhotovitele

Návrh a implementace škálování AGW pro vyšší výkon a dostupnost bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem.

Zhotovitel provede výkonnostní monitoring stávajících přístupových bran AGW a na základě naměřených výsledků navrhne konkrétní způsob zvýšení výkonu přístupových bran.

Jelikož jsou nyní obě brány (interní a externí) každá provozovány pouze na jednom serveru, bude minimálně doporučeno přidat ke každé bráně další server pro zajištění vysoké dostupnosti. Za tímto účelem bude objednatel muset zajistit potřebný hardware a patrně bude nezbytné zajistit odpovídající HW balacing na úrovni infrastruktury nebo jiný obdobný způsob (po odsouhlasení), tak aby byla možná realizace vysoké dostupnosti na úrovni AGW.

Objednatel bude muset poskytnout síťový loadbalancer, který bude zajišťovat rovnoměrné rozdělování požadavků mezi oba servery interní i externí brány. Balancer bude muset být zároveň schopen detekovat nedostupnost jednoho serveru AGW, aby směřoval požadavky na druhý, živý server AGW.

Centrální adresář eDirectory je již provozován v režimu vysoké dostupnosti a zde nepředpokládáme žádné navýšování hardwaru.

Nicméně upozorňujeme Objednatele, že pro potřeby provozu ve vysoké dostupnosti je potřeba řešit vysokou dostupnost i na infrastrukturní úrovni.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo navýšení původního stavu, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí (například pro operační systém), pokud to tato funkcionality bude vyžadovat.

Vývoj autentizační metody podle specifikace EIDAS do AGW

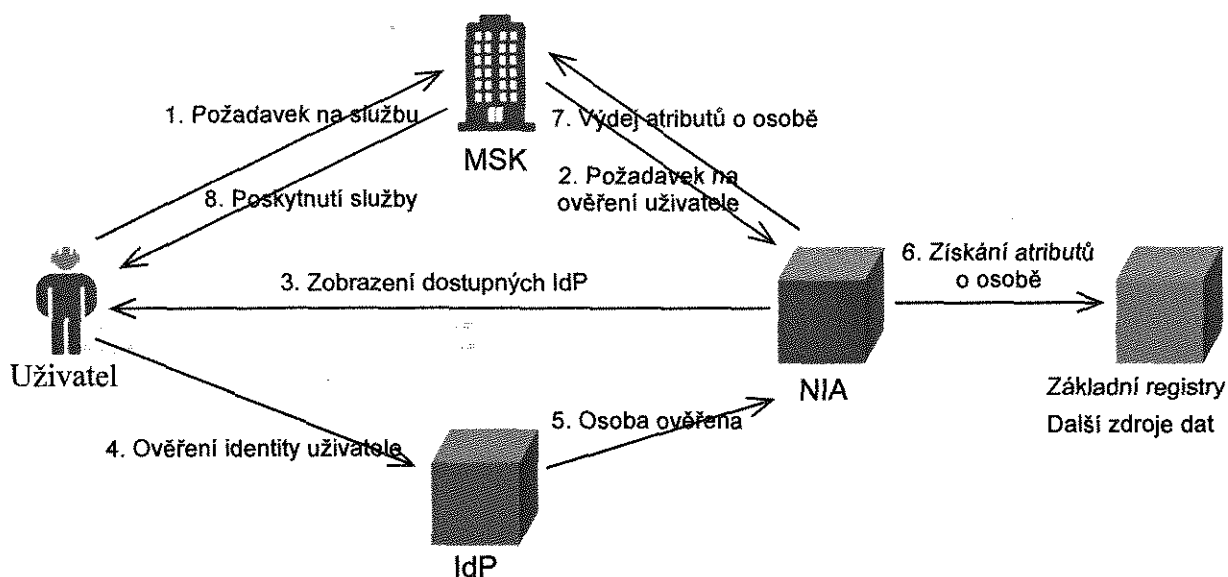
Zhotovitel doplní do autentizačních metod AGW bran autentizační metodu podle specifikací eIDAS tak, abycho byli schopni:

- napojit AGW bránu na národní identitní autoritu za účelem ověření uživatelů,

Závazná detailní technická specifikace zhotovitele

Úprava brány AGW bude splňovat výše uvedené požadavky objednatele, a to následujícím způsobem.

Bude implementována funkcionality, kdy MSK vystupuje vůči NIA jako poskytovatel služeb. Tedy cílem je ověřit přístupujícího uživatele do systémů MSK podle eIDAS, a sice tímto způsobem:



1. Uživatel požaduje po MSK určitou službu (přístup do informačního systému).
2. MSK musí ověřit identitu uživatele. Proto kontaktuje NIA s požadavkem na ověření uživatele.
3. NIA nabídne uživateli seznam poskytovatelů identit, kteří jsou ve vztahu s NIA.
4. Uživatel zvolí příslušného poskytovatele identit a provede u něj ověření své osoby.
5. V případě úspěšného ověření předá identity provider do NIA autentizační token obsahující tzv. IdP pseudonym. Tento pseudonym jednoznačně identifikuje danou osobu v rámci kombinace NIA a poskytovatel identit.
6. NIA nasbírá atributy identity uživatele z ISZR (mimo jiné se zjišťuje úmrtí dané osoby).
7. NIA předá do přístupové brány AGW MSK tzv. SeP pseudonym a množinu všech nasbíraných atributů o identitě dané osoby. Tento pseudonym jednoznačně identifikuje danou osobu v rámci kombinace NIA + MSK jako poskytovatel služby.
8. Byl-li uživatel úspěšně ověřen, umožní AGW MSK uživateli využít jím poptávanou službu.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo navýšení původního stavu, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí (například pro operační systém), pokud to tato funkcionality bude vyžadovat.

Vytvoření testovacího prostředí

Zhotovitel ve spolupráci s objednatelem navrhne a vybuduje testovací prostředí. Implementace testovacího prostředí bude zahrnovat a umožňovat:

- účelem testovacího prostředí je ověření funkčnosti a dopadů na systém správy identit při integraci nových informačních systémů,
- návrh celkové architektury testovacího prostředí, protokolů a síťových postupů, komunikační matice,
- definici zajištění bezpečnosti testovacího prostředí (přístup, šifrování, apod.),
- návrh potřebného SW pro testovací prostředí - specifikace licencí a maintenance,
- vlastní implementace testovacího prostředí v síti MSK a předání k užívání,
- definici pravidel pro používání testovacího prostředí a popis provedení implementace, řešení

- možnost napojení nových systémů na testovací prostředí IDM.

Závazná detailní technická specifikace zhotovitele

Testovací prostředí bude vytvořeno podle výše uvedených požadavků objednatele, s výjimkou řešení nemožnosti klonovat některé systémy, a to následujícím způsobem.

V rámci požadavku budou pouze zprovozněny pouze servery agwi2, sync2, a idm server bez dalších vazeb na ostatní systémy.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo virtuálních strojů pro testovací servery, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí.

Navrhovaná specifikace testovacího prostředí vychází ze současného stavu řešení IDM na KÚ MSK. Aktuálně je řešení IDM provozováno na pěti virtuálních serverech - agwe2, agwi2, idm, idm2 a sync2.

Pro testovací prostředí navrhujeme použití stejný počet virtuálních serverů. Navrhujeme vytvořit testovací prostředí naklonováním produkčních serverů. Výjimkou by byl server idm, u kterého by byla provedena ruční instalace a následná migrace dat z produkčního prostředí.

Hrubý harmonogram vybudování testovacího prostředí je následující:

- Naklonování a úprava DB
- Naklonování serverů agwi2, sync2 a instalace serveru idm (požadována součinnost MSK),
- Rekonfigurace serverů na úrovni OS (např. síťová konfigurace)
- Konfigurace testovací eDirectory a IDM
- Konfigurace testovacího AGW pro připojení na testovací aplikace realizované v rámci projektu
- Konfigurace testovacího serveru SYNC pro systémy realizované v rámci projektu
- Konfigurace testovacího serveru PUMA pro systémy realizované v rámci projektu
- Otestování a předání testovacího prostředí

Po MSK bude požadována součinnost v podobě zajištění potřebného hardwaru, zajištění licencí a přípravy síťové infrastruktury (poskytnutí rozsahu IP adres, zajištění síťových postupů, síťové oddělenosti apod.) a ostatních systémů.

V rámci budování testovacího prostředí nebude řešena problematika nemožnosti klonovat některé systémy, neboť tento požadavek je popsán velmi stručně, obecně a s neměřitelným cílem.

Objednatel musí poskytnout součinnost v podobě dodání hardwaru nebo navýšení původního stavu, dodání nakonfigurovaného síťového prostředí a odpovídajících licencí (například pro operační systém), pokud to tato funkcionality bude vyžadovat.

Customizace auditních reportů

- analýza současného stavu logování,
- návrh řešení a specifikace úprav logování,
- každá komponenta systému pro správu identit bude schopna ukládat detailní auditní informace o operacích s identitami - kdo, co, kdy, výsledek,

Závazná detailní technická specifikace zhotovitele

Bude provedena analýza současného způsobu logování a budou zmapovány všechny vytvářené log soubory.

Log záznamy budou obsahovat tuto strukturu:

- Datum
- Čas
- Výsledek operace
- Operace
- Identifikátor Actora
- Příznak automatizovanosti - JOB/Uživatel/Synchronizace
- Zdroj
- Cíl
- Volný text (volitelně)



Definice pojmů

1. Informační systém je soubor technického vybavení (servery, komunikační infrastruktura, uživatelská pracoviště a jiné) programové vybavení (operační systémy, databázové a aplikační programové vybavení a jiné).
2. Podporované programové vybavení (dále jen „SW“) je soubor programů, jejichž funkčnost podporuje servisní pracoviště zhotovitele.
3. Aktualizace programového a technického vybavení (Update Service, technická podpora systému správy identit) představuje předání nových verzí SW modulů programového vybavení s vylepšenými funkcemi tak, jak je výrobce dává k dispozici. Aktualizace zajišťují kompatibilitu s ostatními SW komponenty informačního systému v souvislosti s jejich vývojem.
4. Místo instalace je pracoviště, kde je instalováno podporované programové vybavení nebo technické vybavení nebo jeho část.
5. Servisní pracoviště zhotovitele provádí všechny potřebné úkony směřující k rychlému odstranění zjištěných potíží a k zajištění provozuschopnosti podporovaného SW.
6. Nahlášení požadavku je úkon, kterým kontaktní pracovníci objednatele sdělí kontaktnímu místu (systému technické a záruční podpory), že nastaly provozní problémy u SW vybavení, které není možné odstranit vlastními silami objednatele a který proto žádá o poskytnutí technické podpory. Konkrétní kategorii požadavku určuje objednatel na základě dohody o kategoriích požadavků mezi objednatelem a zhotovitelem.
7. Odezva je první reakce kontaktního místa (systému technické a podpory) na požadavek objednatele pro poskytnutí podpory.
8. Zprovoznění technického vybavení je uvedení technického vybavení do stavu, ve kterém vykazuje provozní vlastnosti specifikované výrobcem.
9. Servisní zásah se označuje jako činnost, která směřuje k odstranění oznámených provozních potíží.
10. Incident je událost, která způsobuje či může způsobovat neplánované přerušení nebo omezení kvality dodávané služby.
11. Změna je žádost ze strany objednatele o zajištění technické a záruční podpory při využití služby.
12. Požadavek je incident nebo změna.
13. Provozní doba podpory zhotovitele je doba, po kterou je poskytována podpora uživatelům služby zhotovitelem. Provozní doba podpory pro tuto smlouvu je sjednána v rozsahu 5 x 12, tj. v pracovní dny od 7:00 do 19:00.
14. Doba vyřešení je čas od okamžiku předání požadavku zhotoviteli do okamžiku jeho vyřešení, je také měřitelný (součást systému technické a záruční podpory).
15. BD Bussines Day/ pracovní den Po-Pá vyjma oficiálních státních svátků.
16. NBD Next Bussines Day / následující pracovní den.

Rozsah technické podpory

Technická podpora bude obsahovat minimálně služby odstraňování vad, technologický

a legislativní upgrade, servis - podpora provozu, konzultace - hot line.

Odpovědnost za vady

1. Zhotovitel zaručuje, že dílo má vlastnosti a funkční specifikace stanovené touto smlouvou a že je způsobilé pro použití ke sjednanému či obvyklému účelu.
2. Objednatel má právo uplatnit formou reklamace svoje práva z odpovědnosti zhotovitele za vady na kterékoliv části předmětu plnění.
3. Vady (reklamace) budou hlášeny zhotoviteli prostřednictvím Service Desku KÚ.
4. Veškeré vady (reklamace) je objednatel povinen uplatnit u zhotovitele bez zbytečného odkladu poté, kdy vadu zjistil. Nahlášení vady je možné 24 hodin denně 7 dnů v týdnu po celou dobu záruční doby specifikované v tomto článku smlouvy. Zhotovitel bude řešit daný požadavek v době provozní podpory zhotovitele.
5. Objednatel umožní zhotoviteli zabezpečený vzdálený přístup do své datové sítě z IP adresy zhotovitele protokolem TCP/IP za účelem plnění této smlouvy k případným servisním zásahům.

Service Desk KÚ

1. Service Desk KÚ je centrálním místem pro sběr a vyřizování požadavků a tvoří základ systému řízení IT služeb. Systém umožňuje zadávání a evidenci požadavků uživatelů služby v režimu 7*24*365. Na KÚ je implementován Service Desk Fama společnosti Tesco SW. Závady (incidents) budou zaznamenávány v Service Desku KÚ.
2. Zhotovitel provede na své náklady obousměrnou integraci svého systému (Service Desku zhotovitele) se Service Deskem KU, tj. přejímání požadavků ze Service Desku KÚ do svého Service Desku a zpětné poskytování informací o stavu řešení požadavků do Service Desku KÚ. Komunikace mezi Service Desky bude probíhat formou e-mailových notifikací. Service Desk KÚ musí být schopen zasílat do Service Desku zhotovitele e-maily s kompletním textem požadavků včetně příloh. Service Desk KÚ musí být schopen přijímat e-maily s řešením od Service Desku zhotovitele a musí být schopen přiřadit je odpovídajícímu požadavku.
3. Uživatelé služby
 - a) Ze strany zřizovatele:
 - Správci ICT služeb, kteří řeší požadavky zadané uživateli do Service Desku.
 - Zaměstnanci kraje zařazení do krajského úřadu, členové zastupitelstva kraje, členové komisí a výborů, kteří mají právo zadávat požadavky do Service Desku.
 - b) Ze strany organizací:
 - Zaměstnanci organizací, kteří mají právo zadávat požadavky do Service Desku.

Definice SLA (Service Level Agreement)

1. Kategorizace vad a doby řešení:

Kategorie „Vysoká“ je kritická vada, která znemožňuje funkčnost informačního systému a práci uživatelům.

Za kritickou vadu je považován takový stav, kdy nelze spustit informační systém jako celek nebo některou z jeho částí. Informační systém vůbec neplní ani své základní funkcionality, nelze vůbec pracovat, nebo se nelze do systému přihlásit, nebo nelze vkládat data, nebo

není k dispozici standardní uživatelské rozhraní systému.

Maximální nedostupnost informačního systému je 24 hodin za kalendářní měsíc z důvodu řešení kritických vad v provozní době podpory zhotovitele.

Kategorie „Střední“ je vážná vada, která znemožňuje práci uživatelům informačního systému. Za odstranění vady se považuje i nalezení náhradního postupu, nebo řešení, které zajistí funkčnost minimálně ve stejné úrovni.

Za vážnou vadu se považuje stav informačního systému, kdy fungují chybně nebo zcela nefungují některé funkce Informačního systému. Nejsou zobrazována očekávaná data, probíhá nekorektně předávání dat (ať už v rámci systému samotného či v rámci integrace se systémem třetích stran), nefunguje vyhledávání, výstupy poskytují navzájem nekonzistentní výsledky, atp.

Kategorie „nízká“ je drobná vada, která komplikuje práci uživatelům Informačního systému. Za odstranění vady se považuje i nalezení náhradního postupu, nebo řešení, které zajistí funkčnost minimálně ve stejné úrovni.

Drobné vady nemají zásadní vliv na používání Informačního systému. Jedná se o vizuální nesrovnalosti systému či vizualizaci dat, např. zjištěné překlapy, chybné zobrazení diakritiky, chybné seřazení údajů, apod.

Kategorie	Odezva	Doba vyřešení
Vysoká	4 hodiny	8 hodin
Střední	8 hodin	2 pracovní dny
Nízká	2 pracovní dny	5 pracovních dnů

Garantovaná reakční doba k nástupu k servisnímu zásahu bude při nahlášení požadavku (chyby) provedené v režimu 5 x 12 do 12 hodin pracovního dne se počítá od 12 hodin tohoto dne, při nahlášení požadavku provedené po 12 hodině pracovního dne se počítá od 8.00 následujícího pracovního dne.

2. SLA změny dokumentace:

Provedené změny musí zanést zhotovitel do příslušné dokumentace do 10 pracovních dnů po jejich provedení, pokud má umožněn přístup k aktuální dokumentaci.



Příloha č. 3 – Cena

Tabulka č. 1 – Cena za Realizaci díla

Realizace	Cena bez DPH v Kč	Sazba DPH v %	Cena s DPH v Kč
Rozšíření geografické multilicence PUMA IAM Advanced Edition pro neomezený počet uživatelů v rámci Moravskoslezského kraje.	6.330.555,- Kč	21%	7.659.971,55 Kč
Zpracování a předání analýzy a prováděcího návrhu úprav a rozvoje systému správy identit v rozsahu dle technické specifikace uvedené v příloze č. 1 této smlouvy.	216.000,- Kč	21%	261.360,- Kč
Úprava portálu samoobslužného řešení	360.000,- Kč	21%	435.600,- Kč
Rozšíření IDM o workflow modul	504.000,- Kč	21%	609.840,- Kč
Systém zasílání logů do SIEM	216.000,- Kč	21%	261.360,- Kč
Typová instalace a konfigurace otevřeného vzorového konektoru (vzor pro HR systémy)	288.000,- Kč	21%	348.480,- Kč
Specifikace integračního rozhraní pro integraci aplikací	324.000,- Kč	21%	392.040,- Kč

Úprava systému rolí, propagace rolí	648.000,- Kč	21%	784.080,- Kč
Škálování AGW pro vyšší výkon a dostupnost	72.000,- Kč	21%	87.120,- Kč
Vývoj autentizační metody podle specifikace EIDAS do AGW	324.000,- Kč	21%	392.040,- Kč
Vytvoření testovacího prostředí	108.000,- Kč	21%	130.680,- Kč
Customizace auditních reportů	108.000,- Kč	21%	130.680,- Kč
Celková cena za části díla v rámci realizace díla dle čl. III odst. 2.1 této smlouvy	9.498.555,- Kč	21%	11.493.251,55 Kč

Tabulka č. 2 Cena za poskytování Technické podpory

Rutinní provoz – technická podpora	Cena bez DPH v Kč za 12 měsíců	Sazba DPH v %	Cena s DPH v Kč za 12 měsíců	Cena celkem bez DPH v Kč za 60 měsíců
Technická podpora	360.330,58 Kč	21%	436.000,- Kč	1.801.652,90 Kč

Tabulka č. 3 Cena za poskytování dalších služeb

Objednatel předpokládá odebrání následujícího rozsahu plnění v rámci Provozní části díla (rutinní provoz) v každém jednom roce: Školení 50 hodin/rok, Konzultační práce 100 hodin/rok, Programátorské práce 100 hodin/rok.

Rutinní provoz – Další služby	Cena za 1 hodinu bez DPH v Kč	Sazba DPH v %	Cena za 1 hodinu včetně DPH v Kč	Cena celkem za požadovaný počet hodin v Kč s DPH za 1 rok	Cena celkem za požadovaný počet hodin v Kč s DPH za 5 let
Školení	900,- Kč	21%	1.089,- Kč	54.450,- Kč	272.250,- Kč
Konzultační práce	900,- Kč	21%	1.089,- Kč	108.900,- Kč	544.500,- Kč
Programátorské práce	900,- Kč	21%	1.089,- Kč	108.900,- Kč	544.500,- Kč
Cena celkem za požadovaný počet hodin (Školení, Konzultační práce,				272.250,- Kč	1.361.250,- Kč

Programátorské práce)					
-----------------------	--	--	--	--	--

Tabulka č. 4 Nabídková cena celkem, tj. součet cen za plnění dle tabulky č. 1, č. 2.

Realizace + rutinní provoz (za 60 měsíců)	Cena bez DPH v Kč	Sazba DPH v %	Cena celkem s DPH v Kč
Celková nabídková cena za části díla v rámci Realizace díla a Rutinní provoz (Technická podpora a poskytování dalších služeb) v délce 60 měsíců	11.300.207,90 Kč	21%	13.673.251,56 Kč

Příloha č. 4 – Podrobný položkový rozpis všech nutných licencí SW

1x PUMA IAM Advanced Edition upgrade na unlimited uživatelů (geo licence pro Moravskoslezský kraj)

Příloha č. 5 – Seznam poddodavatelů

Zhotovitel neplánuje využití poddodavatelů pro plnění této smlouvy.