

**Smlouva o poskytnutí IDM řešení
(dále též „Smlouva“)**

Smluvní strany:

Česká republika – Ministerstvo zemědělství

se sídlem: Těšnov 17, 110 00 Praha 1

IČ: 00020478

bankovní spojení: ČNB, Praha 1, č. účtu: 1226-001/0710

zastoupená: Davidem Šetinou, ředitelem Odboru správy centrálních informačních systémů
a kybernetické bezpečnosti

(dále jen „Objednatel“ nebo též „Zadavatel“)

číslo smlouvy Objednatele: S2015-0055, č. sml. DMS: 670-2015-13310

a

J3AG, s.r.o.

se sídlem: Průběžná 2397/76, 100 00 Praha 10,

IČ: 03438635, DIČ: CZ03438635

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C,
vložka 231643

bankovní spojení: Fio banka, a.s.č. účtu: 2000680586/2010

zastoupená: Ing. Lukášem Lojkem, MBA, PMP, jednatelem

(dále jen „Zhotovitel“ nebo též „Dodavatel“)

dnešního dne uzavřely tuto smlouvu v souladu s ustanovením § 1746 odst. 2 ve spojení s § 2586 a násl. a s použitím § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“).

Touto Smlouvou se realizuje veřejná zakázka malého rozsahu ve smyslu ust. § 10 a ust. § 12 odst. 3 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.

Obě smluvní strany, vědomy si svých závazků v této smlouvě obsažených a s úmyslem být touto Smlouvou vázány, se dohodly na následujícím znění smlouvy:

1. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

- 1.1.1 je ústředním orgánem státní správy, jehož působnost a zásady činnosti jsou stanoveny zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů,
- 1.1.2 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Zhotovitel prohlašuje, že:

- 1.2.1 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené,
- 1.2.2 ke dni uzavření této Smlouvy není vůči němu vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „insolvenční zákon“), a zavazuje se Objednatele bezodkladně informovat o hrozícím úpadku, popř. o vzniku úpadku jeho společnosti, stejně jako o změnách v jeho kvalifikaci, kterou prokázal v rámci své nabídky na plnění Veřejné zakázky v dále uvedeném smyslu,
- 1.2.3 je subjektem oprávněným k poskytování Maintenance, jak je Maintenance definována v odst. 2.3.2 této Smlouvy, a to po dobu uvedenou taktéž v odst. 2.3.2 této Smlouvy, a Zhotovitel dále prohlašuje, že ke dni uzavření této Smlouvy má uzavřen smluvní dokument platný po celou dobu účinnosti této Smlouvy a opravňující Zhotovitele poskytnout Objednateli Maintenance, ledaže by tohoto smluvního dokumentu nebylo třeba z toho důvodu, že by Maintenance byla poskytována k Free Software/Open Source Software, jak je tento software definován v odst. 9.11 této Smlouvy; v tom případě se Zhotovitel zavazuje postupovat v souladu s příslušnými licenčními ustanoveními pro tento druh software. Zhotovitel se zavazuje zajistit a za stejných podmínek jako u sebe doložit Objednateli, že příslušná oprávnění mají i případní subdodavatelé Zhotovitele.

2. PŘEDMĚT A ÚČEL SMLOUVY

- 2.1. Účelem této Smlouvy je implementace nového identity management (dále jen „IDM“) systému, který má nahradit současné IDM řešení provozované v prostředí Ministerstva zemědělství.
- 2.2. Zhotovitel touto Smlouvou garantuje Objednateli splnění zadání uvedeného v Technické specifikaci v příloze č. 3 této Smlouvy (dále též „TS“) a všech z toho vyplývajících podmínek a povinností. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:
 - 2.2.1. v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel vyjádřený v TS,

- 2.2.2. v případě chybějících ustanovení této Smlouvy budou použita dostatečně konkrétní ustanovení TS,
- 2.2.3. v případě jakéhokoliv rozporu mezi obsahem přílohy č. 1 této Smlouvy a obsahem TS má přednost obsah TS.
- 2.3. Zhotovitel se zavazuje provést pro Objednatele dílo spočívající v závazku Zhotovitele:
- 2.3.1. realizovat pro Objednatele kompletní dodávku IDM systému, která odpovídá specifikaci v příloze č. 1 této Smlouvy a TS, přičemž realizace zahrnuje analýzu, instalaci, implementaci, akceptační testy, dokumentaci, školení a poskytnutí Objednateli časově neomezené licence k užívání IDM systému (dále jen „Poskytnutí IDM řešení“);
- 2.3.2. poskytovat následnou technickou podporu standardních (generických) softwarových produktů tvořících součást IDM systému, včetně zajištění technické podpory ze strany subjektu, který pro daný produkt zastřešuje vývoj a údržbu, tedy zejména opravy chyb, testování nových verzí (dále jen „Poskytovatel Maintenance“), a to dle parametrů uvedených v této Smlouvě, zejména v TS a v katalogovém listu IDM02 Maintenance uvedeném ve Specifikaci katalogových listů v příloze č. 2 této Smlouvy (dále též „Maintenance“) na dobu jednoho (1) roku od splnění etapy Instalace uvedené v Harmonogramu plnění (jak je tento pojem definován v odst. 3.1);
- 2.3.3. poskytovat následnou technickou a metodickou podporu (dále též „Podpora“) dle parametrů uvedených v této Smlouvě, zejména v TS a v katalogových listech vyjma katalogového listu Maintenance ve Specifikaci katalogových listů v příloze č. 2 této Smlouvy (dále též „SKL“), a to od akceptace části Díla spočívající v Poskytnutí IDM řešení bez výhrad, nebo, stanoví-li tak Objednatel, od akceptace části Díla spočívající v Poskytnutí IDM řešení s výhradami, po dobu stanovenou v Harmonogramu plnění;
- (Poskytnutí IDM řešení, Maintenance a Podpora dále společně jen „Dílo“).
- 2.4. Zhotovitel se zavazuje a zaručuje, že veškeré činnosti a věcná plnění, které mají být provedeny na základě této Smlouvy, budou provedeny řádně a v dohodnutých termínech se znalostí a péčí, kterou je možné očekávat od odborníků, kteří mají požadované znalosti a relevantní zkušenosti s realizací činností obdobných jako je předmět této Smlouvy. Dílo nebude obsahovat žádné vady, které by bránily jeho použití k obvyklým účelům.
- 2.5. Zhotovitel se zavazuje v rámci plnění podle této Smlouvy nainstalovat nejnovější, Zhotovitelem otestovanou a doporučenou verzi programových prostředků, která bude v době plnění Smlouvy uvedena na trh.
- 2.6. Objednatel se zavazuje zajistit nezbytnou součinnost za podmínek stanovených v odst. 6.1 této Smlouvy a poskytnuté plnění za podmínek stanovených v této Smlouvě převzít a zaplatit za něj dohodnutou cenu v souladu s platebními podmínkami uvedenými v čl. 5. této Smlouvy.

3. TERMÍNY A MÍSTO PLNĚNÍ

- 3.1. Zhotovitel a Objednatel se dohodli na termínech plnění, které jsou uvedeny v harmonogramu plnění uvedeném v příloze č. 4 této Smlouvy (dále též „Harmonogram plnění“).
- 3.2. Zhotovitel je oprávněn plnit i před sjednaným termínem plnění.
- 3.3. Zhotovitel se zavazuje dodat nejpozději do konce etapy B4. Instalace, definované v Harmonogramu plnění v příloze č. 4 této Smlouvy, veškeré podklady potvrzující uhrazení ceny za licence a Maintenance na dobu jednoho (1) roku za Objednatele a podklady potřebné k následnému obnovení Maintenance. Dále pak Zhotovitel Objednateli předá poklady pro zajištění přístupu k podpoře Poskytovatele Maintenance, aktualizací IDM systému a dalším zdrojům, ke kterým má Objednatel oprávněný přístup na základě platné Maintenance IDM řešení.
- 3.4. Místem plnění se sjednává sídlo Objednatele a Hostingová centra (dále též „HC“) dle odst. 3.5 této Smlouvy. Pokud to povaha plnění této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Zhotovitel oprávněn poskytovat část svého plnění, resp. vést komunikaci s Objednatelem, telefonicky nebo prostřednictvím elektronické komunikace, případně též prostřednictvím vzdáleného přístupu.
- 3.5. Objednatel je oprávněn v průběhu trvání smluvního vztahu rozšířit nebo změnit poskytovatele a tedy i adresy HC v rámci České republiky. Aktuální adresy HC jsou:
 - 3.5.1. Hostingové centrum Nagano
K Červenému dvoru 25/3156
130 00, Praha 3 – Strašnice
 - 3.5.2. Hostingové centrum Chodov
V lomech 2339/1
149 00 Praha 4 – Chodov

4. PROVÁDĚNÍ, PŘEDÁNÍ A PŘEVZETÍ DÍLA

- 4.1. Způsob provedení části Díla spočívající v Poskytnutí IDM řešení bude blíže specifikován v rámci etapy analýza, blíže specifikované v příloze č. 1 této Smlouvy a TS (dále jen „Analýza“).
- 4.2. Dílo provedené Zhotovitelem dle této Smlouvy bude Objednateli předáváno v souladu s postupem uvedeným v tomto čl. 4 Smlouvy. Částí Díla se rozumí: (i) Poskytnutí IDM řešení, (ii) Maintenance a (iii) Podpora.
- 4.3. Část Díla Poskytnutí IDM řešení bude Objednateli předána v místě plnění ve smyslu čl. 3 této Smlouvy v rámci akceptačního řízení, po odsouhlasení a následném potvrzení akceptačního protokolu pověřenými oprávněnými pracovníky Objednatele dle této Smlouvy. Řádné poskytování částí Díla Maintenance a Podpora bude potvrzováno prostřednictvím písemných dokumentů uvedených v odst. 4.6 až 4.8 této Smlouvy. Pro předání a převzetí částí Díla dále platí následující zásady:
 - 4.3.1. proces akceptačního řízení je rozveden dále v tomto článku Smlouvy;

- 4.3.2. Objednatel není povinen část Díla převzít, dokud není předána v souladu s touto Smlouvou. Za takto nedokončenou část Díla není Objednatel povinen zaplatit cenu sjednanou ve Smlouvě.
- 4.4. Akceptační řízení části Díla spočívající v Poskytnutí IDM řešení probíhá následujícím způsobem:
- 4.4.1. Zhotovitel předá příslušnou část Díla Objednateli k akceptačnímu řízení spolu se Zhotovitelem podepsaným předávacím protokolem osvědčujícím předání části Díla k akceptačnímu řízení. Objednatel je povinen převzít část Díla k akceptačnímu řízení a odevzdat Zhotoviteli Objednatelům podepsaný předávací protokol bez zbytečného odkladu. Pro vyloučení pochybností se má za to, že akceptační řízení je zahájeno dnem podpisu předávacího protokolu Objednatelům.
- 4.4.2. Objednatel je povinen ve lhůtě dvanácti (12) pracovních dnů od zahájení akceptačního řízení uvést své výhrady a připomínky k části Díla vyjadřující případné vady části Díla, tj. rozpor vlastností části Díla oproti dohodnuté specifikaci uvedené v této Smlouvě a akceptované Analýze nebo určené v souladu s ní, a to formou písemného soupisu těchto výhrad a připomínek v akceptačním protokolu. V akceptačním protokolu Objednatel též specifikuje, zda část Díla v důsledku zjištěných vad neakceptuje, nebo jí akceptuje s výhradou odstranění zjištěných vad, přičemž Objednatel je rovněž oprávněn v případě akceptace části Díla s výhradou uvést v předmětném akceptačním protokolu část ceny v procentech z celkové ceny za část Díla, kterou bude možné dle odst. 5.8 této Smlouvy fakturovat, a to s ohledem na rozsah vad části Díla, které budou důvodem pro odmítnutí akceptace části Díla s výrokem „Akceptováno bez výhrad“. Objednatel není povinen akceptovat část Díla s výhradou.
- 4.4.3. V případě, že Objednatel na části Díla neshledá žádné vady, část Díla akceptuje a vystaví o tom písemný akceptační protokol, ve kterém uvede, že část Díla je akceptována bez výhrad, a který bez zbytečného odkladu doručí Objednateli.
- 4.4.4. Neakceptoval-li Objednatel část Díla bez výhrad, je Zhotovitel povinen se ve lhůtě pěti (5) dnů od doručení akceptačního protokolu vyjádřit k Objednatelům zjištěným vadám, tyto bez zbytečného odkladu, nejpozději však do deseti (10) dnů od neúspěšné akceptace, odstranit a předat část Díla k opakovanému akceptačnímu řízení dle tohoto odst. 4.4 Smlouvy. Pokud z důvodu oprávněných výhrad Objednatelů nebude dodržen termín pro akceptaci části Díla bez výhrad, je Zhotovitel v prodlení.
- 4.4.5. Část Díla bude považována za provedenou jako celek a předanou Objednateli dnem podpisu akceptačního protokolu Objednatelům s výrokem „Akceptováno bez výhrad“.
- 4.4.6. Pro vyloučení pochybností je stanoveno, že akceptační řízení ohledně akceptace části Díla (Poskytnutí IDM řešení) proběhne po úspěšném ukončení akceptačních testů, dodání dokumentace, poskytnutí školení a provedení veškerých dalších dílčích částí této části Díla, nedohodnou-li se smluvní strany jinak.

- 4.5. Pro akceptaci Analýzy ve smyslu odst. 4.1 této Smlouvy se přiměřeně použije akceptační procedura uvedená v odst. 4.4 této Smlouvy, nedohodnou-li se strany jinak. Ujednání o možnosti fakturovat část ceny se neaplikují.
- 4.6. Zhotovitel zašle Objednateli vždy do pěti (5) pracovních dnů ode dne uplynutí kalendářního měsíce, ve kterém byla poskytována Podpora, ke schválení záznam o poskytnutí služeb dle SKL dle katalogového listu IDM04 „Reparametrizace a optimalizace“ s identifikací poskytnutých činností včetně jejich pracnosti (dále jen „Záznam o poskytnutí služeb dle KL Reparimetrizace a optimalizace“). V Záznamu o poskytnutí služeb dle KL Reparimetrizace a optimalizace bude rozpad proveden dle nejmenší časové jednotky, hodina na jednoho člověka, pro dokladování pracnosti, a to nejméně v této míře detailu: konkrétní fyzická osoba provádějící činnost, popis činnosti, datum činnosti a doba trvání činnosti, přičemž evidovanou a účtovanou časovou jednotkou je každá započatá hodina činnosti. Plnění poskytované v rámci KL Reparimetrizace a optimalizace bude vždy považováno za poskytnuté poté, co Objednatel potvrdí jeho řádné poskytnutí podpisem Záznamu o poskytnutí služeb dle KL Reparimetrizace a optimalizace.
- 4.7. Zhotovitel po uplynutí každého kalendářního měsíce poskytování Podpory vyhotoví kompletní výkazy, ze kterých bude jednoznačně zřejmé, zda byly služby Podpory a Maintenance poskytovány dle parametrů stanovených v příloze č. 2 této Smlouvy (dále jen „Report podpory“); pro vyloučení pochybností Report podpory zahrnuje údaje uváděné v Záznamu o poskytnutí služeb dle KL Reparimetrizace a optimalizace. Součástí Reportu podpory bude rovněž vyhodnocení výše slevy z ceny, na kterou vzniklo Objednateli právo za vyhodnocovací období, za které byl Report podpory vyhotoven.
- 4.8. Zhotovitel zašle Objednateli vyhotovený Report podpory vždy do pěti (5) pracovních dnů ode dne uplynutí kalendářního měsíce, který je vyhodnocovacím / měřicím obdobím popsáním v předmětném Reportu podpory. Report podpory podléhá písemnému schválení Objednatel. Pokud do desátého (10) dne ode dne předložení Reportu podpory nedojde k jeho schválení Objednatel, zavazují se strany zahájit v dobré víře jednání za účelem dosažení shody o obsahu Reportu podpory.
- 4.9. Strany se dohodly, že použití ustanovení § 2605 odst. 2 občanského zákoníku je pro tuto Smlouvu vyloučeno.

5. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

- 5.1. Cena Díla byla stanovena dohodou v souladu s ustanoveními zákona č. 526/1990 Sb. o cenách, ve znění pozdějších předpisů následovně v (Kč):

Položka č.	Předmět plnění	Cena v Kč bez DPH	Sazba DPH v %	Výše DPH v Kč	Cena v Kč s DPH
1.	Poskytnutí IDM řešení	393000	21	82530	475530
2.	Maintenance za období jednoho roku	10000	21	2100	12100
3.	Podpora vyjma Reparimetrizace a	3916,67	21	822,50	4739,17

Položka č.	Předmět plnění	Cena v Kč bez DPH	Sazba DPH v %	Výše DPH v Kč	Cena v Kč s DPH
4.	optimalizace – měsíční cena Podpora vyjma Reparametrizace a optimalizace – cena za období jednoho roku	47000	21	9870	56870
5.	Reparametrizace a optimalizace – cena za 1 člověkohodinu, (viz. SKL IDM04)	125	21	26,25	151,25
6.	Reparametrizace a optimalizace – cena za 20 člověkodní, (viz. SKL IDM04)	20000	21	4200	24200
Celková nabídková cena (součet položek 1., 2., 4. a 6.)		470000	21	98700	568700

- 5.2. Celková cena Díla bude určena jako součet cen za (i) Poskytnutí IDM systému, (ii) Maintenance za období jednoho roku a (iii) Podporu dle doby jejího poskytování v souladu s Harmonogramem plnění. Sjednaná celková cena pro celý rozsah Díla, určená v souladu s první větou tohoto odst. 5.2 této Smlouvy, je cenou nejvýše přípustnou, která je platná po celou dobu plnění této Smlouvy. Celkovou cenu Díla, určenou v souladu s první větou tohoto odst. 5.2 této Smlouvy, není možné z žádného důvodu navýšit s výjimkou navýšení sazby DPH při změně právních předpisů. Celková cena Díla, určená v souladu s první větou tohoto odst. 5.2 této Smlouvy, je stanovena za Dílo v rozsahu specifikace uvedené v této Smlouvě. Jakékoliv změny ceny Díla mohou být provedeny pouze dodatkem k této Smlouvě, který může být sjednán pouze v souladu s ustanoveními zákona č. 137/2006 Sb., o veřejných zakázkách ve znění pozdějších právních předpisů. Bude-li Podpora poskytována pouze po dobu části měsíce, bude hrazena poměrná část měsíční ceny. Zhotoviteli nevzniká právní nárok na poskytnutí plnění/ceny v plném rozsahu položky 6. tabulky v odst. 5.1. a tím ani na poskytnutí plné ceny. V rámci KL Reparametrizace a optimalizace budou hrazeny pouze reálně čerpané člověkohodiny, resp. jejich části odpovídající čerpaným člověkohodinám, podle sjednané sazby za člověkohodinu a to do maximálního objemu definovaného tímto katalogovým listem.
- 5.3. Cena zahrnuje ocenění všech prací a dodávek, které je nezbytné provést na základě vymezení dle této Smlouvy a jejích příloh, zejména přílohy č. 1, TS a SKL, není-li současně ve Smlouvě stanoveno, že jejich provedení má zajistit v rámci své součinnosti Objednatel.
- 5.4. Cena za část Díla Poskytnutí IDM řešení bude zaplácena Objednatelem na základě daňového dokladu (faktury), který Zhotovitel vystaví v souladu s touto Smlouvou po akceptaci části Díla Poskytnutí IDM řešení bez výhrad. V případě akceptace části Díla Poskytnutí IDM řešení s výhradou bude postupováno podle

- odst. 5.8 níže. Paušální měsíční cena za Podporu vyjma KL Reparametrizace a optimalizace bude hrazena za každý ukončený měsíc Podpory na základě daňového dokladu vystaveného Zhotovitelem po schválení Reportu podpory. Cena za Podporu bude zohledňovat případnou výši slevy z ceny dle SKL. Cena za poskytování plnění dle KL Reparametrizace a optimalizace bude hrazena za každý ukončený měsíc na základě schváleného Záznamu o poskytnutí služeb dle KL Reparametrizace a optimalizace. Tato cena bude stanovena násobkem Zhotovitelem vynaložených a Objednatelem schválených člověkodnů, resp. jejich částí odpovídajících čerpaným člověkohodinám, a ceny za jednu člověkohodinu dle odst. 5.1. Objednatel není povinen čerpat ani uhradit maximální počet člověkohodin, resp. člověkodnů dle KL Reparametrizace a optimalizace. Cena za Maintenance bude uhrazena ročně na základě faktury Zhotovitele. Zhotovitel je oprávněn vystavit první fakturu po zahájení poskytování Maintenance.
- 5.5. Faktury Zhotovitele musí obsahovat všechny náležitosti řádného daňového a účetního dokladu v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, zejména dle jeho § 29, číslo této Smlouvy, číslo Smlouvy DMS, číslo projektu Objednatele, identifikaci plnění dle této Smlouvy, přičemž v případě faktury za Poskytnutí IDM řešení její nedílnou přílohou je závěrečný akceptační protokol o akceptaci části Díla bez výhrad podepsaný Objednatelem, nejde-li o fakturu dle odst. 5.8 níže. V případě faktury za poskytování Podpory je nedílnou přílohou Objednatelem schválený Report podpory. V případě faktury za poskytování Maintenance je přílohou faktury Objednatelem potvrzený protokol o řádném zahájení poskytování Maintenance za příslušné období. V případě faktury za poskytování služeb dle KL Reparametrizace a optimalizace je přílohou faktury Objednatelem schválený Záznam o poskytnutí služeb dle KL Reparametrizace a optimalizace obsahující údaj o množství reálně vynaložených člověkohodin na tyto služby.
- 5.6. Pokud faktura neobsahuje všechny zákonem a Smlouvou stanovené náležitosti a přílohy, je Objednatel oprávněn ji do data splatnosti vrátit s tím, že Zhotovitel je poté povinen vystavit novou fakturu s novým termínem splatnosti.
- 5.7. Splatnost faktur je dohodou smluvních stran stanovena na 30 dnů (třicet) ode dne jejího prokazatelného doručení Objednateli. Zaplacením se pro účely této Smlouvy rozumí odepsání příslušné částky z účtu Objednatele ve prospěch účtu Zhotovitele.
- 5.8. Objednatel neposkytuje zálohy. V případě, že Objednatel akceptuje Poskytnutí IDM řešení s výhradou, lze akceptační protokol prokazující takovouto akceptaci použít pro fakturaci do 60% ceny Poskytnutí IDM řešení, stanoví-li tak písemně Objednatel. Zbývající část ceny Poskytnutí IDM řešení bude použita jako zádržné a bude vyplacena na základě daňového dokladu, jehož přílohou bude akceptační protokol prokazující akceptaci Poskytnutí IDM řešení bez výhrad.
- 5.9. Jeden (1) člověkodén představuje osm (8) člověkohodin, tedy osm (8) hodin práce jednoho pracovníka.

6. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

- 6.1. Smluvní strany jsou povinny se vzájemně informovat o všech okolnostech důležitých pro řádné a včasné provedení Díla, přičemž Objednatel je povinen poskytnout Zhotoviteli součinnost v následujícím rozsahu:
 - 6.1.1. zajistit potřebné přístupy do prostor MZe pro pracovníky Zhotovitele a spolupráci pracovníků MZe se Zhotovitelem v nezbytném rozsahu,
 - 6.1.2. poskytnout Zhotoviteli všechny nezbytné součinnosti pro provedení Díla, které si Zhotovitel vyžádá a takovou nezbytnost součinnosti ze strany Objednatele náležitě odůvodní (zejména, fyzický přístup k hardware, přístupová práva nebo asistenci oprávněné osoby – administrátora IT),
 - 6.1.3. vyjadřovat se k návrhům na další postup Zhotovitele, bude-li to nezbytné pro řádné zhotovení Díla,
 - 6.1.4. zajistit účast svých pracovníků na školení v dohodnutém termínu,
 - 6.1.5. zajistit připravenost hardware, který má Objednatel poskytnout dle TS.
- 6.2. Objednatel je povinen poskytovat součinnost pouze v nezbytném rozsahu, který je specifikován v odst. 6.1 této Smlouvy. Součinnost bude poskytnuta prostřednictvím kontaktní osoby.
- 6.3. V případě, že je nezbytná součinnost Objednatele pro řádné plnění této Smlouvy Zhotovitelem a Objednatel je v prodlení s jejím poskytnutím, zavazuje se Zhotovitel na toto prodlení Objednatele písemně upozornit v přiměřených intervalech, které nebudou delší než 5 dnů.
- 6.4. Zhotovitel je povinen Objednatele neprodleně informovat o jakýchkoliv okolnostech, které mohou ohrozit realizaci Díla nebo způsobit zpoždění realizace Díla.
- 6.5. Objednatel má právo přesvědčit se kdykoliv v průběhu plnění Díla o stavu prací na Díle. Pokud by se ukázalo, že Zhotovitel práce na Díle neprovádí nebo je prokazatelně a bezdůvodně provádí v rozporu se zadáním, má právo od Smlouvy odstoupit, a to za předpokladu, že na tento rozpor Zhotovitele písemně upozornil a Zhotovitel ve lhůtě deseti (10) pracovních dnů nesjednal nápravu tohoto stavu.
- 6.6. Zhotovitel je povinen provádět Dílo prostřednictvím osob, které uvedl v seznamu členů odborného týmu za účelem prokázání kvalifikace v rámci své nabídky na plnění Veřejné zakázky. Zhotovitel je povinen prostřednictvím těchto osob provádět etapy Analýza, Poskytnutí IDM řešení a Podpora. Zhotovitel je oprávněn nahradit tyto osoby jinými osobami s obdobnou kvalifikací s předchozím písemným souhlasem Objednatele. Objednatel neodepře udělení souhlasu bez závažného důvodu.
- 6.7. Zhotovitel je oprávněn použit pro plnění svých závazků subdodavatele uvedené v příloze č. 7 této Smlouvy, není-li v této Smlouvě, zejména v jejím odst. 6.6., stanoveno jinak. Jiné subdodavatele je Zhotovitel oprávněn použít pro plnění svých závazků, pokud s použitím subdodavatele Objednatel udělil svůj písemný souhlas

- 6.8. Zhotovitel se při plnění zavazuje dodržovat zásady bezpečnosti informací v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“), a vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen „vyhláška o kybernetické bezpečnosti“). Bezpečností informací se v souladu se zákonem o kybernetické bezpečnosti rozumí zajištění důvěrnosti, integrity a dostupnosti informací, které budou uchovávány, vytvářeny nebo zpracovávány v implementovaném IDM systému nebo v systémech, které mají vazbu na implementovaný IDM systém a v souvislosti s kterými Objednateli vznikají právní povinnosti na základě zákona o kybernetické bezpečnosti (§ 3 tohoto zákona).
- 6.9. Zhotovitel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené zákonem o kybernetické bezpečnosti, vyhláškou o kybernetické bezpečnosti, vyhláškou č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Zejména se Zhotovitel zavazuje poskytnout Objednateli součinnost směřující k zavedení a provádění bezpečnostních opatření podle uvedených právních předpisů.
- 6.10. Jestliže vznikne v souvislosti se zavedením a prováděním bezpečnostních opatření podle právních předpisů uvedených v předchozím odstavci potřeba uzavřít dodatek k této smlouvě nebo zvláštní smlouvu, zavazuje se Zhotovitel poskytnout veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy, a k uzavření takového dodatku, resp. smlouvy.
- 6.11. Rozsah a povaha součinnosti Zhotovitele sjednané v odst. 6.8 až 6.10 Smlouvy budou vždy určeny zejména podle rozsahu a povahy vlivu implementovaného IDM systému na bezpečnost informací Objednatele a rovněž podle rozsahu a povahy vazeb implementovaného IDM systému na systémy, v souvislosti s kterými Objednateli vznikají právní povinnosti na základě zákona o kybernetické bezpečnosti (§ 3 tohoto zákona).
- 6.12. Zhotovitel je povinen zajistit dodržování pravidel a pokynů Objednatele týkajících se vstupu a pohybu osob v místech plnění uvedených v čl. 3. osobami jeho pracovníků a pracovníků jeho subdodavatelů.
- 6.13. V případě, že po skončení účinnosti této Smlouvy dojde k uzavření nové smlouvy týkající se služeb Podpory nebo jakékoli jejich části nebo podobného či souvisejícího plnění s novým poskytovatelem odlišným od Zhotovitele, zavazuje se Zhotovitel po skončení účinnosti této Smlouvy poskytovat Objednateli nebo jím určeným třetím stranám veškerou součinnost potřebnou pro účely plynulého a řádného poskytování služeb obdobných službám Podpory či jejich příslušné části novým poskytovatelem, pokud bude naplnění tohoto cíle záviset na znalostech Zhotovitele získaných na základě plnění této Smlouvy. Pro vyloučení pochybností se uvádí, že Zhotovitel je v rámci součinnosti dle tohoto odstavce Smlouvy povinen zabezpečit na výzvu Objednatele osobní účast příslušných členů realizačního týmu na jednáních s Objednatelem či jím určenými třetími stranami. Zhotovitel se zavazuje tuto součinnost poskytovat s odbornou péčí, bez

zbytečného odkladu a zodpovědně, a to minimálně po dobu tří (3) měsíců ode dne, ve kterém tato Smlouva zanikla. Zhotovitel se zavazuje reagovat na požadavek Objednatele nebo jím určené třetí strany a zahájit poskytování součinnosti dle tohoto odstavce Smlouvy nejpozději do tří (3) pracovních dnů ode dne doručení takového požadavku. Smluvní strany se dohodly, že cena za plnění dle tohoto odstavce je součástí ceny za poskytování služeb Podpory bez nároku na další finanční plnění.

6.14. Použije-li Zhotovitel při plnění této smlouvy subdodavatele, odpovídá Objednateli, jakoby plnil sám.

7. ZÁRUKA A ZÁRUČNÍ SERVIS

7.1. Zhotovitel se zavazuje v délce jednoho roku poskytovat technickou podporu Poskytovatele Maintenance za podmínek uvedených v SKL. Maintenance je Zhotovitel v plném rozsahu a na svoji odpovědnost povinen zajistit i v případě, že součástí Díla bude instalace Open Source Software ve smyslu odst. 9.6 této Smlouvy.

7.2. Zhotovitel poskytuje záruku za jakost spočívající v tom, že Zhotovitel se zavazuje v průběhu jednoho roku ode dne akceptace části Díla Poskytnutí IDM řešení bez výhrad („záruční doba“) odstranit na své náklady veškeré vady části Díla Poskytnutí IDM řešení, kterými se rozumí zejména Zhotovitelem zaviněná nemožnost použití části Díla Poskytnutí IDM řešení v souladu s jeho účelem nebo rozpor jeho vlastností v s příslušnou dokumentací, a to do dvaceti (20) pracovních dnů (za podmínky, že Objednatel poskytne nezbytnou součinnost, zejména přístup na pracoviště, kde je částí Díla Poskytnutí IDM řešení instalováno nebo využíváno, součinnost administrátora). Tato záruční doba se prodlužuje o dobu, po kterou nelze částí Díla Poskytnutí IDM řešení využívat. Záruka dle tohoto článku se nevztahuje na vady způsobené zásahem Objednatele nebo jím pověřené třetí osoby do Díla provedeným bez vědomí Zhotovitele. Pro vyloučení pochybností se uvádí, že záruka za jakost uvedená v tomto odst. 7.2 se vztahuje i na implementovaný IDM systém ve verzi upravené v rámci poskytování Maintenance nebo Podpory. Závazkem dle odst. 7.2 této Smlouvy nejsou dotčeny závazky týkající se poskytování Maintenance nebo Podpory. Zhotovitel dále poskytuje záruku za jakost oprav nebo úprav provedených v průběhu záruční doby s tím, že záruční doba vztahující se k úpravám nebo opravám provedeným v průběhu záruční doby uplyne sto osmdesát (180) dnů po ukončení záruční doby vztahující se k části Díla Poskytnutí IDM řešení jako celku.

8. SMLUVNÍ POKUTY A NÁHRADA ŠKODY

8.1. Za každý den prodlení Zhotovitele s provedením části Díla Poskytnutí IDM řešení (jako celku) je Zhotovitel povinen zaplatit Objednateli smluvní pokutu ve výši 0,2% z částky určené jako celková nabídková cena bez DPH uvedené v odst. 5.1 této Smlouvy.

8.2. Za každý den prodlení Zhotovitele s odstraněním faktické vady části Díla Poskytnutí IDM řešení v intencích odst. 7.2. této Smlouvy je Zhotovitel povinen

zaplatit Objednateli smluvní pokutu ve výši 0,2% z maximální celkové ceny Díla bez DPH uvedené v odst. 5.2 této Smlouvy.

- 8.3. Za každý den prodlení Zhotovitele se splněním povinnosti poskytnout Objednateli:
- 8.3.1. podklady potvrzující uhrazení ceny za licence a Maintenance na dobu jednoho (1) roku,
 - 8.3.2. podklady pro zajištění přístupu k podpoře Poskytovatele Maintenance, aktualizacím implementovaného IDM systému a dalším zdrojům, ke kterým má Objednatel oprávněný přístup na základě platné Maintenance implementovaného IDM systému,
- a to do konce etapy B.4. Instalace definované v Harmonogramu plnění v příloze č. 4 této Smlouvy, je Zhotovitel povinen zaplatit Objednateli smluvní pokutu ve 2.000,- Kč.
- 8.4. Zhotovitel je povinen uhradit Objednateli smluvní pokutu ve výši 400.000,- Kč za každé porušení povinnosti mlčenlivosti nebo jiné povinnosti specifikované v čl. 11. Smlouvy či jakékoli povinnosti specifikované v čl. 9. Smlouvy, a to za každý jednotlivý případ porušení povinností.
- 8.5. V případě, že Zhotovitel nevyužije pro plnění svých závazků v rozporu s odst. 6.6 osobu tam uvedenou, ale bude své závazky plnit prostřednictvím jiných osob, uhradí smluvní pokutu ve výši 50.000,- Kč, a to za každý jednotlivý případ takového porušení.
- 8.6. V případě porušení pravidel uvedených v čl. 6. odst. 6.11. této Smlouvy se Zhotovitel zavazuje uhradit Objednateli smluvní pokutu ve výši 50.000,- Kč, a to za každý jednotlivý případ takového porušení.
- 8.7. Objednatel má právo na slevu z ceny nebo uhrazení smluvní pokuty v souladu s ustanoveními přílohy č. 2 této Smlouvy.
- 8.8. Zhotovitel nese plnou odpovědnost za to, že Dílo nebude zatíženo právem třetí osoby. V případě, že jakákoliv třetí strana uplatní jakékoliv nároky vůči Objednateli z důvodu porušení obchodního tajemství, patentu, autorských či jiných práv duševního vlastnictví třetích stran souvisejících s provedením Díla, Objednatel bez zbytečného odkladu písemně oznámí Zhotoviteli tento uplatněný nárok či jakoukoli žalobu v této věci podanou proti Objednateli, nejpozději však ve lhůtě dvaceti (20) pracovních dnů ode dne, kdy třetí strana uplatnila nárok vůči Objednateli, resp. Objednateli byla doručena žaloba třetí strany. V případě soudního sporu nebo rozhodčího řízení se Zhotovitel zavazuje na výzvu Objednatele poskytnout veškerou potřebnou součinnost, a to především podat Objednateli veškeré informace, které jsou nezbytné k prokázání práv a Objednatele, resp. Zhotovitele, dále předat Objednateli včas listinné důkazy a navrhnout svědky, kteří mohou být vyslechnuti před soudem. Zhotovitel se zavazuje odškodnit Objednatele v plné výši v případě, že třetí strana úspěšně a oprávněně proti Objednateli uplatní autorskoprávní či jiný nárok plynoucí z právní vady poskytovaného Díla.
- 8.9. Smluvní strany odpovídají za způsobenou škodu v rámci platných právních předpisů a této Smlouvy. Zhotovitel plně odpovídá též za škodu způsobenou

v souvislosti s touto smlouvou svým subdodavatelem. Žádná ze smluvních stran není odpovědná za škodu nebo prodlení způsobené okolnostmi vylučujícími odpovědnost ve smyslu § 2913 občanského zákoníku. Zhotovitel odpovídá za skutečně vzniklou škodu a ušlý zisk.

- 8.10. Objednatel je oprávněn požadovat náhradu škody i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta nebo sleva z ceny, přičemž smluvní strany výslovně uvádí, že uhrazení smluvní pokuty ani slevy z ceny nemá vliv na právo na náhradu škody.
- 8.11. Smluvní pokuty jsou splatné jednadvacátý (21.) den ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší. Zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky.
- 8.12. Zhotovitel se zavazuje mít platné a účinné pojištění odpovědnosti za škodu způsobenou Zhotovitelem třetím osobám ve výši 2.500.000,- Kč a udržovat toto pojištění po celou dobu realizace Díla, zajišťování Podpory a trvání záruky k Dílu.

9. AUTORSKÁ PRÁVA, LICENČNÍ UJEDNÁNÍ A PŘECHOD VLASTNICTVÍ

- 9.1. Pro případ, že výsledkem činnosti Zhotovitele a/nebo jeho subdodavatele či osob jimi využitými k poskytování plnění dle této Smlouvy je dílo, které naplňuje znaky díla dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů (dále jen „autorské dílo“):
 - 9.1.1. Zhotovitel prohlašuje, že bude nejpozději ke dni zahájení jakéhokoli užívání autorského díla Objednatelem oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorskému dílu a že má nebo bude mít nejpozději k uvedenému dni souhlas autorů k uzavření následujících licenčních ujednání; toto prohlášení zahrnuje i taková práva autorů, která by vytvořením autorského díla teprve vznikla. Pokud prohlášení dle předchozí věty nebude moci být dodrženo z důvodu, že část autorského díla byla provedena subdodavatelem Zhotovitele, je Zhotovitel povinen zajistit si od subdodavatele dostatečná práva k poskytnutí licence a souvisejících oprávnění Objednateli v souladu s ustanoveními této Smlouvy, a to nejpozději ke dni převzetí příslušné subdodávky;
 - 9.1.2. Zhotovitel poskytuje Objednateli (nabyvateli licence) oprávnění ke všem v úvahu přicházejícím způsobům užití autorského díla a bez jakéhokoliv omezení, a to zejména pokud jde o územní, časový nebo množstevní rozsah užití;
 - 9.1.3. smluvní strany se výslovně dohodly, že cena za poskytnutí této licence Zhotovitele je již zahrnuta v ceně za poskytnutí Díla;
 - 9.1.4. Zhotovitel poskytuje tuto licenci Objednateli (nabyvateli licence) jako nevýhradní. Tímto ustanovením není dotčeno oprávnění Objednatele dle níže uvedených ustanovení udělit sublicence, resp. postoupit licenci dalším osobám;

- 9.1.5. Objednatel není povinen licenci využít;
- 9.1.6. Objednatel (nabyvatel licence) je oprávněn práva tvořící součást licence zcela nebo zčásti jako podlicenci poskytnout třetí osobě;
- 9.1.7. Objednatel (nabyvatel licence) je oprávněn bez dalšího upravit či jinak měnit autorské dílo, jeho název nebo označení autorů, stejně jako spojit autorské dílo s jiným dílem nebo zařadit autorské dílo do díla souborného nebo na jeho základě či při jeho využití vytvořit dílo nové, a to přímo nebo prostřednictvím třetích osob, přičemž tato oprávnění trvají i po ukončení účinnosti Smlouvy.
- 9.2. Pokud v rámci plnění této Smlouvy vzniknou zdrojové kódy počítačových programů, je Zhotovitel povinen předat Objednateli tyto zdrojové kódy, které jsou spustitelné v prostředí Objednatele, zaručující možnost ověření, že zdrojový kód je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace a komentáře zdrojového kódu (dokumentovaný a komentovaný zdrojový kód). Zhotovitel je povinen předat Objednateli zdrojové kódy bez prodlevy, nejpozději do tří (3) pracovních dnů, po jejich vyvinutí a doručení žádosti Objednatele o jejich poskytnutí, nejpozději však do pěti (5) pracovních dnů po skončení účinnosti Smlouvy, a to na základě předávacího protokolu.
- 9.3. Pokud kdykoliv po dobu trvání Smlouvy dojde k opravě zdrojového kódu v souvislosti s plněním této smlouvy, jeho změně, doplnění, upgrade či update, předá Zhotovitel, a to bez vyzvání, tento nový dokumentovaný a komentovaný zdrojový kód Objednateli neprodleně, nejpozději do tří (3) pracovních dnů, po změně, opět na základě předávacího protokolu.
- 9.4. Předchozí ustanovení tohoto článku se v plném rozsahu vztahují pouze na autorská díla, která byla vytvořena Zhotovitelem a/nebo jeho subdodavateli či osobami jimi využitými k poskytování plnění na základě této Smlouvy (dále jen „Unikátní díla“). Zhotovitel je povinen Objednateli poskytnout nebo pro Objednatele zajistit práva užití autorská díla, která nejsou Unikátními díly, ale představují standardní software třetích stran, tedy softwarové vybavení dodané v rámci Smlouvy, které nebylo vyvinuto Zhotovitelem a není aplikační softwarovou komponentou vyvinutou v rámci Smlouvy (dále jen „Neunikátní díla“), v rozsahu standardní licence umožňující minimálně užívání implementovaného IDM systému v souladu s jeho určením, přičemž teritoriální rozsah poskytnuté licence musí být sjednán alespoň pro území České republiky a licence musí být poskytnuta jako nevypověditelná minimálně na dobu trvání autorských práv majetkových. Pro vyloučení jakýchkoliv pochybností smluvní strany sjednávají, že jakákoliv autorská díla poskytnutá Objednateli v rámci plnění dle této Smlouvy jsou Unikátními díly, nejsou-li Zhotovitelem předem a výslovně označena za Neunikátní díla. Použití jakéhokoliv Neunikátního díla Zhotovitelem v rámci plnění dle této Smlouvy podléhá předchozímu písemnému schválení ze strany Objednatele. Ve vztahu k dokumentaci vztahující se k Neunikátním dílům je Zhotovitel povinen poskytnout nebo pro Objednatele zajistit práva duševního vlastnictví přiměřeně dle odst. 9.4 a 9.5 Smlouvy.

- 9.5. Aniž jsou tím dotčena jiná oprávnění Objednatele dle této Smlouvy, platí, že veškerá autorská díla poskytnutá Objednateli jako součást plnění poskytovaného dle Smlouvy je Objednatel oprávněn, bez nutnosti opatřit si další souhlas Zhotovitele či jiné osoby, poskytnout k užití a případným úpravám či jiným změnám všem organizačním složkám státu a příspěvkovým organizacím v rezortu Objednatele, právníkům osobám založeným a/nebo řízeným Objednatelem a dalším osobám, kterým bude podle rozhodnutí Objednatele umožněno užití implementovaného IDM systému. Objednatel je dále oprávněn, bez nutnosti opatřit si další souhlas Zhotovitele či jiné osoby, poskytnout těmto subjektům podlicenci nebo na ně licenci postoupit, a to dle své volby. Možnost poskytnutí licence nebo sublicence dle předchozí věty se nepoužije pro Neunikátní díla, u nichž je předmětné nakládání s Neunikátním dílem vyloučeno standardními licenčními podmínkami vykonavatele majetkových práv autorských k předmětnému Neunikátnímu dílu. Zhotovitel je však při předání Neunikátního díla, jehož licenční podmínky omezují Objednatele v poskytnutí podlicence nebo postoupení licence, povinen předem písemně na tuto skutečnost Objednatele upozornit. Pokud Zhotovitel Objednatele na předmětnou skutečnost takto neupozorní, odpovídá za veškerou újmu, která může být Objednateli a/nebo všem organizačním složkám státu, příspěvkovým organizacím a právníkům založeným a/nebo řízeným Objednatelem způsobena. Bez ohledu na jiná ustanovení této Smlouvy platí, že licenční oprávnění poskytnutá Objednateli na základě této Smlouvy nesmí omezovat Objednatele v poskytnutí implementovaného IDM systému k užití jiným osobám uvedeným v první větě tohoto odstavce, ani nesmí omezovat Objednatele v zajišťování provozu a rozvoje implementovaného IDM systému jiným dodavatelem než je Zhotovitel, to vše ani tehdy, budou-li součástí implementovaného IDM systému Neunikátní díla.
- 9.6. Zhotovitel tímto prohlašuje a Objednateli garantuje, že ani po ukončení účinnosti této Smlouvy nebo po ukončení plnění ze strany Zhotovitele nebude Zhotovitel uplatňovat žádné nároky v souvislosti s užíváním Unikátních i Neunikátních děl Objednatelem nebo třetími osobami ani úpravami či jinými změnami Díla prováděnými Objednatelem nebo třetími osobami. Zhotovitel dále prohlašuje a výslovně Objednatele ujišťuje, že na základě práv poskytnutých Zhotovitelem bude Objednatel oprávněn poptávat služby údržby, podpory a rozvoje implementovaného IDM systému nebo podobná či související plnění u jiných dodavatelů v budoucích zadávacích řízeních dle zákona č. 137/2006 Sb., o veřejných zakázkách ve znění pozdějších předpisů (dále jen „ZVZ“), resp. v zadávacích řízeních dle budoucích předpisů upravujících zadávání veřejných zakázek. V případě, že jakákoliv osoba namítne porušení svého práva duševního vlastnictví v souvislosti s postupem Objednatele dle předchozí věty, je Zhotovitel povinen na své náklady zajistit poskytnutí veškerých potřebných práv Objednateli.
- 9.7. V případě, že výsledkem plnění dle této Smlouvy budou jiné předměty duševního vlastnictví než autorská díla, poskytne Zhotovitel Objednateli licenci a další práva duševního vlastnictví s obdobnou specifikací jako v případě autorských děl.
- 9.8. Cena za poskytnutí všech práv duševního vlastnictví dle Smlouvy, zejména dle tohoto článku, je plně zahrnuta v ceně Díla dle čl. 5. Smlouvy.

- 9.9. Smluvní strany se dohodly, že ustanovení § 2364, § 2370 a § 2378 občanského zákoníku se nepoužijí.
- 9.10. Bude-li v souvislosti s plněním předmětu této Smlouvy Zhotovitelem vytvořena databáze, bude se za pořizovatele takové databáze vždy považovat Objednatel.
- 9.11. Je-li k užití předmětu plnění dle této Smlouvy nezbytná instalace software s otevřeným zdrojovým kódem (tzv. Free Software/Open Source Software), který umožňuje neomezené provádění změn ve zdrojovém kódu a tím i ve vlastním softwaru, dále jen „Open Source Software“, platí následující ujednání:
- 9.11.1. Použití jakéhokoliv Open Source Software Zhotovitelem v rámci plnění této Smlouvy podléhá předchozímu písemnému schválení ze strany Objednatele, přičemž Zhotovitel je povinen předem sdělit Objednateli, zda se jedná o software poskytovaný za úplatu nebo bezúplatně.
 - 9.11.2. Nezbytnou podmínkou pro použití Open Source Software Zhotovitelem je, předchozí zajištění Maintenance ve smyslu odst. 7.1. této Smlouvy ze strany Zhotovitele.
 - 9.11.3. Zhotovitel je povinen nejpozději při předání předmětu plnění Objednateli zpracovat a předložit Objednateli přehled Open Source Software s uvedením autora, licenčního modelu, zajištění Maintenance dle odst. 7.1. této Smlouvy a případných omezení, která se na užívání takového software vztahují a dále zdrojové kódy. Přehled podle předchozí věty musí být přiložen k předávacímu protokolu.
 - 9.11.4. Zhotovitel odpovídá za vady předmětu plnění včetně Open Source Software. Zhotovitel zejména odpovídá za funkčnost předmětu plnění jako celku a použitelnost předmětu plnění jako celku pro účely vyplývající z této Smlouvy a jejích příloh.
 - 9.11.5. Zhotovitel odpovídá za to, že Objednatel bude oprávněn užívat Open Source Software v rozsahu nezbytném k plnému využití předmětu plnění dle této Smlouvy a za podmínek uvedených v tomto odst. 9.11 Zhotovitel je povinen nahradit Objednateli veškeré škody a náklady, které by mohly vzniknout v důsledku uplatnění práv třetích osob souvisejících s Open Source Software, který je užit k plnění dle této Smlouvy.
- 9.12. Je-li k užití předmětu plnění dle této Smlouvy nezbytná instalace proprietárního software s uzavřeným kódem distribuovaného bezúplatně (tzv. Freeware), uplatní se přiměřeně pravidla dle odst. 9.11 této Smlouvy, s výjimkou zejména volné šířitelnosti zdrojových kódů, a s přihlédnutím k odstavcům 9.4, 9.5 a 9.6 obecná pravidla o užití standardního SW třetích stran v rámci Neunikátních děl.

10. OZNÁMENÍ A KOMUNIKACE

- 10.1. Veškerá oznámení, tj. jakákoliv komunikace na základě této Smlouvy, bude probíhat v souladu s tímto článkem.
- 10.2. Kromě jiných způsobů komunikace dohodnutých mezi stranami se za účinné považují osobní doručování, doručování doporučenou poštou, faxem či

elektronickou poštou, a to na následující adresy smluvních stran, nebo na takové adresy, které si strany vzájemně písemně oznámí.

10.2.1. Za Objednatele:

Kontakt	Oblast	Telefon	E-mail
David Šetina	Smluvní a obchodní podmínky, včetně podpisu předávacího a akceptačního protokolu	221 813092	david.setina@mze.cz
Ing. Karel Štefl	Technické záležitosti	221 812 659	karel.stefl@mze.cz

10.2.2. Za Zhotovitele:

Kontakt	Oblast	Telefon	E-mail
Lukáš Lojek	Smluvní a obchodní podmínky, včetně podpisu předávacího a akceptačního protokolu	724256039	Lukas.Lojek@J3AG.CZ
Lukáš Lojek	Technické záležitosti	724256039	Lukas.Lojek@J3AG.CZ
Lukáš Lojek	Záruční servis a Podpora	724256039	Lukas.Lojek@J3AG.CZ

10.3. Oznámení se považují za uskutečněná v případě osobního doručování anebo doručování doporučenou poštou okamžikem doručení, v případě posílání faxem či elektronickou poštou okamžikem obdržení potvrzení od protistrany při použití stejného komunikačního kanálu.

10.4. Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny do tří (3) dnů ode dne změny oprávněné osoby na takovou změnu druhou smluvní stranu písemně upozornit. Zmocnění zástupce oprávněné osoby musí být písemné s uvedením rozsahu zmocnění.

11. OCHRANA INFORMACÍ

11.1. Zhotovitel se zavazuje během plnění i po ukončení této Smlouvy zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví v souvislosti s plněním této Smlouvy (dále též „důvěrné informace“).

11.2. Ustanovení odst. 11.1. se nevztahuje na informace, které jsou veřejné nebo které měl Zhotovitel k dispozici nebo mu byly dostupné i před jejich zpřístupněním Objednatelem a na informace, které se staly veřejnými bez toho, aby to protiprávně způsobila přijímající strana, a dále na informace, které Zhotovitel prokazatelně sám vyvinul nebo zjistil bez porušení závazků dle této Smlouvy.

11.3. Porušením ochrany informací není, pokud Zhotovitel zpřístupní důvěrné informace Objednatele:

- 11.3.1. neboť byl povinen učinit tak na základě zákona nebo vykonatelného rozhodnutí soudu či příslušného správního orgánu;
- 11.3.2. svým subdodavatelům, oprávněně se podílejícím na plnění této Smlouvy, jen v nezbytně nutném rozsahu potřebném k zajištění plnění jejich povinností subdodavatele, zavázal-li uvedené osoby smluvně k ochraně těchto informací;
- 11.3.3. svým účetním, daňovým, právním nebo jiným odborným poradcům, jsou-li tyto osoby smluvně nebo zákonem zavázány k ochraně těchto informací.
- 11.4. Zhotovitel se zavazuje v souvislosti s ochranou informací poučit všechny osoby, které se budou podílet na plnění předmětu Smlouvy, a to včetně subdodavatelů, o povinnosti mlčenlivosti.
- 11.5. Smluvní strany jsou povinny zachovávat ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a ZVZ.
- 11.6. Zhotovitel souhlasí se zveřejněním Smlouvy na internetových stránkách Ministerstva zemědělství ČR ve smyslu směrnice MZe č. 6/2015. Zhotovitel je srozuměn s tím, že Objednatel je oprávněn zveřejnit Smlouvu na svých webových stránkách a dále je povinen uveřejnit dle § 147a odst. 1 písm. a) ZVZ na svém profilu zadavatele (dále jen „Profil“), tuto Smlouvu včetně všech jejích změn a dodatků. Dále je Zhotovitel srozuměn s tím, že dle § 147a odst. 1 písm. b) ZVZ je Objednatel povinen uveřejnit na Profilu výši skutečně uhrazené ceny za plnění Veřejné zakázky a dle § 147a odst. 1 písm. c) ZVZ též seznam subdodavatelů Zhotovitele. Zhotovitel tímto uděluje Objednateli souhlas k uveřejnění všech podkladů, údajů a informací uvedených v tomto odstavci a těch, k jejichž uveřejnění vyplývá pro Objednatele povinnost dle právních předpisů.
- 11.7. Bez ohledu na jiná ustanovení této Smlouvy je Objednatel oprávněn v souladu s § 147a ZVZ uveřejnit:
- 11.7.1. tuto Smlouvu včetně všech jejích změn a dodatků,
- 11.7.2. výši skutečně uhrazené ceny za plnění Veřejné zakázky a
- 11.7.3. seznam subdodavatelů dodavatele Veřejné zakázky.
- 12. PLATNOST A ÚČINNOST SMLOUVY, VÝPOVĚĚ A ODSTOUPENÍ OD SMLOUVY**
- 12.1. Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami a je uzavřena na dobu určitou do konce doby poskytování Podpory.
- 12.2. Každá smluvní strana je oprávněna od Smlouvy odstoupit v případech stanovených zákonem a touto Smlouvou.
- 12.3. Objednatel je dále oprávněn od Smlouvy odstoupit v případě, že:
- 12.3.1. je Zhotovitel v prodlení s plněním jeho závazků po dobu delší než 30 dnů;

- 12.3.2. Zhotovitel pozbude oprávnění vyžadované právními předpisy k činnostem, k jejichž provádění se Zhotovitel zavázal podle této Smlouvy;
- 12.3.3. Zhotovitel poruší povinnost ochrany důvěrných informací ve smyslu této Smlouvy;
- 12.3.4. vůči Zhotoviteli bylo zahájeno insolvenční řízení nebo byl insolvenční návrh zamítnut pro nedostatek majetku Zhotovitele, podle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů (dále jen „insolvenční zákon“), nebo pokud Zhotovitel vstoupí do likvidace či se ocitne v úpadku.

12.4. V případě odstoupení od Smlouvy tato Smlouva zaniká ke dni doručení odstoupení druhé smluvní straně. Smluvní strany si vrátí již poskytnuté plnění, není-li touto Smlouvou stanoveno jinak. Odstoupení od Smlouvy se nedotýká částí Díla, které byly ke dni účinnosti odstoupení od Smlouvy dokončeny a předány Objednateli, přičemž Poskytnutí IDM řešení se považuje za jednu část Díla. Objednatel má právo rozhodnout, zda si ponechá rozpracované plnění, tedy část Díla, která nebyla ke dni účinnosti odstoupení od Smlouvy dokončena a předána Objednateli. V případě, že si Objednatel rozpracované plnění ponechá, má Zhotovitel nárok na poměrnou část ceny odpovídající poměrné části zhotoveného Díla. V případě, že Objednatel nebude mít zájem ponechat si rozpracované plnění, má Zhotovitel, nebude-li se jednat o odstoupení od Smlouvy v rámci jejího odst. 12.3 této Smlouvy, nárok na náhradu účelně vynaložených nákladů na provedení daného plnění do doby doručení odstoupení od Smlouvy, výše náhrady těchto nákladů však nesmí být vyšší, než by byla 1/2 výše ceny předmětného plnění ponížené dle předchozí věty.

12.5. Účinky každého odstoupení od Smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této Smlouvy druhé smluvní straně. Odstoupením od Smlouvy nezaniká nárok na náhradu škody vzniklé porušením Smlouvy ani oprávněný nárok na zaplacení smluvních pokut.

12.6. Objednatel je oprávněn tuto Smlouvu částečně vypovědět v části týkající se poskytování Podpory, a to s dvouměsíční výpovědní dobou, která začíná běžet ode dne doručení výpovědi Zhotoviteli.

12.7. Ukončením účinnosti této Smlouvy nejsou dotčeny nároky z odpovědnosti za vady, nároky z odpovědnosti za škodu a nároky ze smluvních pokut, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy. Licence, ostatní práva dle čl. 9 a záruky poskytnuté po dobu účinnosti Smlouvy jsou zachovány v rozsahu, v jakém se týkají plnění, které si v souladu s touto Smlouvou Objednatel ponechá.

13. POSTOUPENÍ A ZMOCNĚNÍ

13.1. Žádná práva ani povinnosti z této Smlouvy nemohou být postoupena jednou smluvní stranou na třetí osobu bez předchozího písemného souhlasu druhé smluvní strany, není-li v této Smlouvě výslovně uvedeno jinak.

- 13.2. Pokud Zhotovitel v souladu s touto Smlouvou pověří plněním některých svých povinností z této Smlouvy třetí osobu, zůstává Zhotovitel plně odpovědný za plnění třetí strany tak, jako by plnil sám.
- 13.3. Zhotovitel není na základě této Smlouvy oprávněn jednat jménem Objednatele bez písemné plné moci udělené pro konkrétní účel specifikovaný v takové plné moci Objednatelem.

14. ZÁVĚREČNÁ USTANOVENÍ

- 14.1. Zhotovitel tímto prohlašuje, že v době uzavření Smlouvy není vůči němu vedeno řízení dle insolvenčního zákona a zavazuje se Objednatele bezodkladně informovat o všech skutečnostech o jeho hrozícím úpadku, popř. o prohlášení jeho úpadku.
- 14.2. Zhotovitel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.
- 14.3. Tato Smlouva (a její přílohy) představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze v souladu s ustanoveními ZVZ písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných osobami oprávněnými jednat jménem smluvních stran.
- 14.4. Vztahy vzniklé mezi smluvními stranami na základě této Smlouvy se řídí občanským zákoníkem a dalšími ustanoveními právních předpisů České republiky, zejména autorským zákonem. Smluvní strany se dohodly, že veškeré spory vzniklé na základě této Smlouvy budou řešeny prostřednictvím obecných soudů České republiky.
- 14.5. Nedílnou součástí této Smlouvy jsou tyto přílohy:
- Příloha č. 1 - Návrh technického řešení
 - Příloha č. 2 - Specifikace katalogových listů
 - Příloha č. 3 - Technická specifikace
 - Příloha č. 4 - Harmonogram plnění
 - Příloha č. 5 - Vzor předávacího protokolu
 - Příloha č. 6 - Vzor akceptačního protokolu
 - Příloha č. 7 - Seznam subdodavatelů
- 14.6. V případě rozporu mezi čl. 1 až 14 této Smlouvy a přílohami mají přednost ustanovení čl. 1 až 14 této Smlouvy. Tím není dotčeno ustanovení odst. 2.2 článku 2. Smlouvy, přičemž garance tam uvedená má před jinými ustanoveními Smlouvy přednost.

- 14.7. Práva Objednatele vyplývající z této Smlouvy či jejího porušení se promlčují ve lhůtě patnácti (15) let ode dne, kdy právo mohlo být uplatněno poprvé.
- 14.8. Zhotovitel přebírá podle § 1765 odst. 2 občanského zákoníku nebezpečí změny okolností v souvislosti s plněním této Smlouvy, zejména v souvislosti s cenou za poskytnuté plnění a požadavky na poskytování Podpory.
- 14.9. Tato Smlouva je vyhotovena ve 4 vyhotoveních v českém jazyce s platností originálu, z nichž každá ze smluvních stran obdrží 2 vyhotovení.
- 14.10. Smluvní strany prohlašují, že si tuto Smlouvu přečetly, rozumí jejímu obsahu a s jejím obsahem souhlasí, což stvrzují svými podpisy.

Za Objednatele:

V Praze/dne 27.1. 2016



Ceská republika –
Ministerstvo zemědělství
David Šetina
Ředitel Odboru správy centrálních
informačních systémů a kybernetické
bezpečnosti

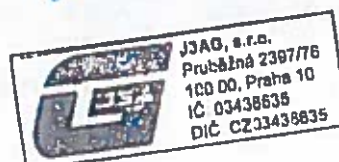
**MINISTERSTVO
ZEMĚDĚLSTVÍ**
Těšnov 65 I
110 00 Praha 1 - Nové Město
-22-

Za Zhotovitele:

V Praze dne 27.1. 2016



J3AG, s.r.o.
Ing. Lukáš Lojek, MBA, PMP
jednatel

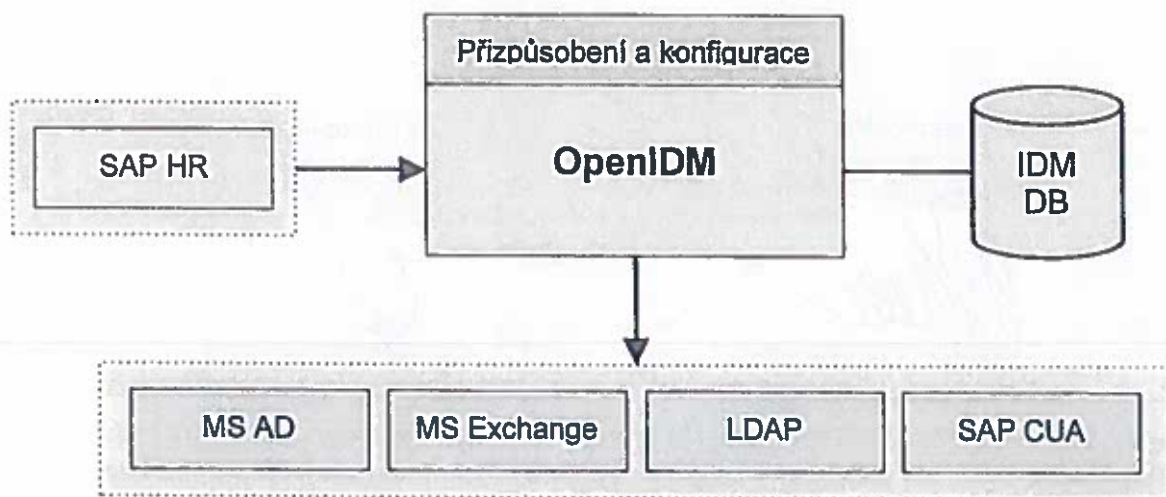


NÁVRH TECHNICKÉHO ŘEŠENÍ

Dodávané řešení je založené na open-source produktu OpenIDM společnosti Forgerock. OpenIDM využívá nejmodernější technologie (OSGi stack, REST JSON, Backbone.JS pro UI, a další) a zároveň i ověřené komponenty svého předchůdce (Sun Identity Manager) v podobě konektorů OpenICF.

Pro zajištění požadovaných funkcionalit je spolu s OpenIDM dodávána nástavba v podobě „Přizpůsobení a konfigurace Orchitech“ (Orchitech Customization) zahrnující vlastní moderní uživatelské rozhraní (s využitím technologií AngularJS, Material Design a dalších) a rozšiřující customizačními skripty (pokročilý Groovy SQL konektor a další).

OpenIDM i přizpůsobení a konfigurace Orchitech odpovídají licenčním podmínkám stanoveným zadavatelem v návrhu smlouvy.



Obr. 1: Logické schéma komponent

Navrhované řešení navazuje na současný stav popsany v kapitole 3 technické specifikace a splní požadavky stanovené v dalších kapitolách dokumentu technické specifikace.

1.1 Návrh technického řešení požadavků k implementaci (5.1)

1.1.1 Obsluha současných základních IDM procesů organizace (5.1)

Požadavek zadavatele:

IDM systém bude instalován a konfigurován v prostředí MZe tak, aby obsluhoval současné základní IDM procesy organizace, zmíněné v odstavci 3.1 (technické specifikace). Tyto procesy budou v rámci analýzy revidovány dodavatelem a jejich finální podobu schválí zadavatel. Účel revize je primárně zjednodušení stávajících procesů, jejichž podoba je částečně ovlivněna možnostmi současného IDM řešení.

Zmiňované procesy Založení nového uživatele, Změna atributů uživatele, Administrátorské uzamčení/odemčení uživatele, Administrátorská aktivace účtů uživatele DPP/DPČ v podobě procesů, v níž jsou uvedeny v Příloze A technické specifikace, představují základní funkčnost systému OpenIDM a jejich implementace bude zajištěna vhodnou konfigurací systému, kterou po revizi procesů uchazeč provede.

1.1.2 Import z HR systému (5 1.1)

Požadavek zadavatele:

Import uživatelů bude realizován načítáním CSV souboru, který bude v pravidelném intervalu exportován SAP HR systémem do vybrané sdílené složky.

Importované osoby/kontrakty jsou celkem čtyř typů:

1. HPP - Hlavní Pracovní Poměr
2. SP – Služební poměr
3. DPČ - Dohoda o Pracovní Činnosti
4. DPP - Dohoda o Provedení Práce

IDM systém bude automaticky zakládat účty v řízených systémech pouze pro kontrakty typu SP a HPP. Jedna osoba může mít maximálně jeden SP nebo HPP, může mít však více poměrů DPČ/DPP. Proto nejsou účty na koncových systémech pro kontrakty typu DPČ/DPP zakládány automaticky, ale jsou pouze (před)vytvořeny v IDM systému a až na základě potvrzení administrátorem je pro takového IDM uživatele vytvořen uživatelský účet ve vybraném řízeném systému (administrátor zvolí v jakých řízených systémech bude účet vytvořen).

V rámci importního procesu je implementován ochranný mechanismus, který přeruší import v případě, že je detekováno příliš velké množství změn, přičemž tento počet je definován jako konfigurovatelný parametr.

Pro načítání CSV souboru bude využit *CSV File* konektor. Tento konektor bude v pravidelných intervalech provádět kontrolu obsahu CSV a pro nové záznamy založí identitu (v terminologii OpenIDM se jedná o tzv. *managed user*). Vazba mezi záznamem v CSV a databázi OpenIDM bude realizována přes vybraný unikátní identifikátor.

Identity založené pro SP nebo HPP budou označeny jako automaticky propagované (v rámci validačních skriptů pro cílové systémy).

Identity pro DPP/DPČ nebudou automaticky propagované a jejich propagaci bude mít možnost manuálně vyvolat oprávněný uživatel v uživatelském rozhraní IDM.

Ochranný mechanismus na detekování velkého počtu změn bude implementován tzv. hookem (nakonfigurovanou obsluhou) v rámci rekonciliačního¹ kontextu synchronizace HR systému a IDM. Tento hook bude mít nastavený povolený počet změn, přičemž přesný mechanismus vyhodnocení změn a určení jejich počtu (absolutní / relativní) musí být součástí analýzy. Jako výchozí návrh předpokládáme, že součet odstraněných, přidaných a jakkoliv změněných záznamů má být menší než nakonfigurovaná konstanta.

¹ Rekonciliace je v terminologii OpenIDM obecnější pojem, je používán i pro porovnávání zdrojového systému s evidencí IDM.

Kromě ochranného mechanismu se samozřejmě počítá se standardní validací, která zajistí, že načítaný CSV soubor obsahuje smysluplný obsah.

1.1.3 Provisioning do řízených systémů (5.1.2)

Požadavek zadavatele:

Uživatelům importovaným do IDM systému jsou provisionovány uživatelské účty do řízených systémů, dle nastavených pravidel, která přímo vycházejí z popsaných procesů.

Provisioning bude implementován tak, aby odpovídal aktuálnímu stavu, popsaném v odstavci 3.3. V rámci dodávky budou tedy napojeny následující 4 systémy:

1. Microsoft Active Directory
2. Microsoft Exchange
3. LDAP (OID)
4. SAP CUA

Před samotným napojením řízených systémů bude provedeno mapování IDM uživatelů na existující uživatelské účty na řízených systémech. Mapování bude probíhat podle jednoznačného uživatelského jména, které je v podobě čísla zaměstnance. Toto mapování bude Objednateli předloženo k revizi a až po jeho schválení bude realizováno v IDM systému.

Integrace na každý z řízených systémů bude podporovat speciální pilotní režim, v rámci kterého nebudou do řízeného systému propagovány žádné změny (budou read-only), budou pouze logovány, tak aby mohla být provedena analýza chování provisioningu a nebyl přítom ohrožen provoz těchto napojených řízených systémů.

Požadované 4 cílové systémy budou integrovány pomocí konektorů OpenICF (LDAP connector, .NET Powershell connector a SAP connector). Tyto konektory umožňují konfiguraci a přizpůsobení pomocí pomocných skriptů dle požadavků zadavatele.

Mapování existujících účtů na identity bude zajištěno za pomoci mechanismu tzv. korelačních skriptů. Tyto skripty umožňují implementaci komplexních pravidel pro propojení existujících účtů s existujícími identitami. Uchazeč navrhne pravidla mapování v rámci analytické fáze.

Rekonciliace objektů v podání OpenIDM je dvoufázová – v první fázi dochází k vyhodnocení synchronizační situace (objekt existuje jen v IDM, objekt existuje jen v cílovém systému, objekty se navzájem liší atp.). V druhé fázi dochází k vykonání předdefinované akce na základě zjištěné situace (update objektu v cílovém systému, smazání objektu v cílovém systému atp.). Jednou z podporovaných akcí je *zalogování zjištěné situace*. Tato funkcionalita bude využita pro implementaci požadavku *pilotního režimu*.

1.1.4 Admin rozhraní (5.1.3)

Požadavek zadavatele:

Dodaný IDM systém bude disponovat webovým administrátorským rozhraním, prostřednictvím kterého bude administrátorům umožněno provádět následující akce:

- Přehled IDM uživatelů, včetně jejich účtů spravovaných na koncových systémech.
- Okamžitá blokáce IDM uživatele, včetně jeho navázaných účtů. Tato blokáce nebude ovlivněna HR importem.
- Aktivace IDM uživatele, který byl zablokován HR importem. Tato aktivace nebude

ovlivněna HR importem.

- Aktivace konkrétního účtu na koncovém systému, který je navázán na neaktivního IDM uživatele. Tato aktivace nebude ovlivněna HR importem.

Veškeré tyto administrátorské akce budou řádně auditovány a budou přeposílány spolu s ostatními auditními logy do systému SIEM (viz další odstavec).

Webové admin rozhraní musí být kompatibilní s prohlížečem:

- **Internet Explorer ve verzi 10 a vyšší.**

Administrační rozhraní bude dostupné v rámci *Přizpůsobení a konfigurace Orchitech*, které obsahuje vlastní uživatelské rozhraní. V rámci tohoto rozhraní je možné procházet identity evidované v OpenIDM a zobrazovat jejich atributy, včetně navázaných objektů (mj. účtů).

Uživatelské rozhraní je implementováno za použití moderních technologií jako tzv. single-page application – HTML5, CSS3, AngularJS, Material Design, JSPM, Babel a dalších. Uživatelské rozhraní je kompatibilní s moderními prohlížeči (Internet Explorer 10 a vyšší, Firefox, Chrome, Opera), včetně zobrazení na mobilních zařízeních (např. tablet).

V rámci detailu identity je v uživatelském rozhraní možné vyvolávat i vybrané operace, jako je aktivace / blokace uživatele a aktivace konkrétního navázaného účtu. Ruční aktivace / blokace bude ukládána v odděleném atributu tak, aby byla nezávislá na stavu přebíraném z HR systému.

Operace prováděné v rámci uživatelského rozhraní jsou logovány v rámci serveru OpenIDM. Konfigurace logování je popsána ve vyjádření k následujícímu bodu.

1.1.5 Integrace se systémem SIEM (5.1.4)

Požadavek zadavatele:

IDM systém loguje jak veškeré aktivity prováděné administrátory, tak i veškeré automatické operace nad uživateli IDM a účty v řízených systémech prováděné IDM systémem. Všechny tyto logované záznamy jsou v reálném čase přenášeny do systému pro bezpečnostní monitoring (SIEM) k jejich vyhodnocení a uložení na centrálním bezpečném místě pro případnou zpětnou analýzu.

Události je možné vyčítat systémem SIEM jednou z následujících metod:

- Syslog
- SNMP TRAP
- Textový soubor
- JDBC
- Microsoft Event Log

Veškeré operace nad daty a spouštěné procesy jsou zaznamenávány v podobě auditních záznamů. Systém pro sběr a zápis auditních záznamů OpenIDM je vysoce konfigurovatelný. Vedle zápisu do databáze je podporován zápis do CSV souboru, zápis přes HTTP request anebo možnost implementace vlastního úložiště. Pro integraci se SIEM jsou relevantní metody zpřístupnění CSV exportů nebo zpřístupnění databáze pro JDBC konektor systému SIEM. Konkrétní způsob bude specifikován v rámci analýzy a nemá vliv na náročnost implementace.

1.1.6 Notifikace (5 1 5)

Požadavek zadavatele:

Součástí IDM systému je notifikační engine, který umožňuje naplánovat mailové notifikace na základě definovaných událostí. Objednatel má k dispozici rozhraní, pomocí kterého může libovolně měnit obsah notifikačních mailů nebo adresátů. Dále je mu umožněno notifikace deaktivovat nebo znovu aktivovat.

V rámci dodávky budou nastaveny následující notifikace:

1. Notifikace o založení nového uživatele do SAP CUA
2. Notifikace o zamknutí účtu v SAP CUA
3. Notifikace o odemknutí účtu v SAP CUA
4. Notifikace o založení IDM uživatele
5. Notifikace o vytvoření nového emailového účtu
6. Notifikace o vytvoření nového účtu v MS AD
7. Notifikace o novém uživateli bez platného manažera
8. Notifikace o odpojení mailboxu

OpenIDM obsahuje službu pro posílání notifikačních e-mailů. Skripty pro obsluhu příslušných událostí budou rozšířeny o odeslání požadovaných notifikačních e-mailů pomocí této služby. Definice e-mailu (obsah, adresáti, aktivace / deaktivace zaslání) bude obsahem nastavení OpenIDM, která je spravovaná administrátory systému.

1.2 Technické řešení požadavků na podporu funkcionality

V této kapitole je popsán způsob, jakým řeší nabízený IDM systém požadavky zadavatele na funkcionalitu. Jak ukazují popisy technického řešení požadavků, jsou tyto nabízeným systémem nativně podporovány.

1.2.1 Správa rolí (5.2.1)

Požadavek zadavatele:

IDM systém umožňuje definovat role, které se skládají ze sady oprávnění v řízených systémech (např. skupiny v LDAPu), nebo ze skupiny jiných rolí (zanořené role). Přiřazením role IDM uživateli, získá uživatel oprávnění v řízeném systému odpovídající sadě oprávnění takové role, případně sady oprávnění všech zanořených rolí. Pokud IDM uživatel nemá žádnou roli, která by mu přiřazovala oprávnění v konkrétním řízeném systému, nebude takový uživatel disponovat aktivním účtem v tomto systému.

Systém umožňuje definovat pravidla, na základě kterých jsou uživatelé automaticky přiřazováni do rolí (resp. odebráni z rolí).

OpenIDM umožňuje definici rolí (*managed role*). Koncept rolí v OpenIDM je vysoce konfigurovatelný a přiřazení role tak může vést k vytvoření účtu, nastavení konkrétního atributu anebo jiné specifické úpravě chování synchronizace do cílového systému.

Pro systémy s vlastními právy je standardním postupem tato práva načítat do OpenIDM (dle konvence jako objekty *managed group*). Role mohou tyto skupiny linkovat a přiřazení role pak určí, které skupiny mají být v systému uživateli přiřazeny.

Pravidla pro validaci synchronizovaného uživatele (pravidla vyhodnocující, který uživatel má právo na účet) pak umožňují definovat podmínky, které účet v cílovém systému dovolí,

pouze pro případ, kdy má uživatel alespoň jednu skupinu (resp. oprávnění) z daného systému.

Díky flexibilnímu datovému modelu OpenIDM (OpenIDM do velké míry nerozlišuje, jaké objekty spravuje a synchronizuje a jaké jsou mezi nimi vazby) je možné model práv libovolně rozšiřovat.

1.2.2 Schvalovací workflow (5.2.2)

Požadavek zadavatele:

Součástí systému je workflow engine, který umožňuje definovat a spouštět schvalovací procesy pro přidělování rolí, případně jiné aktivity. Je možné definovat víceúrovňové schvalování, ve kterém jako schvalovatel figuruje buďto konkrétní uživatel, nebo skupina uživatelů/členové role.

Systém podporuje tzv. automatické schvalování – pokud je žadatel zároveň schvalovatel, není toto schvalování vyžadováno a je automaticky označeno jako schválené.

OpenIDM v sobě zahrnuje pokročilý BPMN 2 workflow engine Activiti. Tento engine podporuje všechny požadované funkcionality.

1.2.3 Uživatelské rozhraní (5.2.3)

Požadavek zadavatele:

IDM systém poskytuje kromě administrátorského rozhraní také webové uživatelské rozhraní umožňující všem IDM uživatelům základní self-service zahrnující:

- Kontrola hodnot vlastních atributů, přiřazených rolí a vlastních řízených účtů
- Podání žádosti o přiřazení role (výběr role z katalogu rolí)
- Změna vlastního hesla (včetně hesel účtů v řízených systémech)

Uživatelé, kteří figurují jako schvalovatelé rolí (vlastník role, security manažer, nadřízený, atp.) mohou v tomto rozhraní provádět navíc akce:

- Schválení/zamítnutí žádosti o roli
- Přehled žádostí ke schválení, včetně těch, které byly již odbavené
- Přehled podřízených uživatelů (atributy, role)

Systém umožňuje řídit oprávnění v rámci webového uživatelského rozhraní IDM systému. V systému lze definovat alespoň následující uživatelské role:

- Administrátor – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému
- Operátor – systém má přístupný na čtení a je mu umožněno několik základních operací nad uživateli (reset hesla, blokace, atp.)
- Uživatel – základní funkce self-service

Webové uživatelské rozhraní musí být kompatibilní s prohlížečem:

- Internet Explorer ve verzi 10 a vyšší.

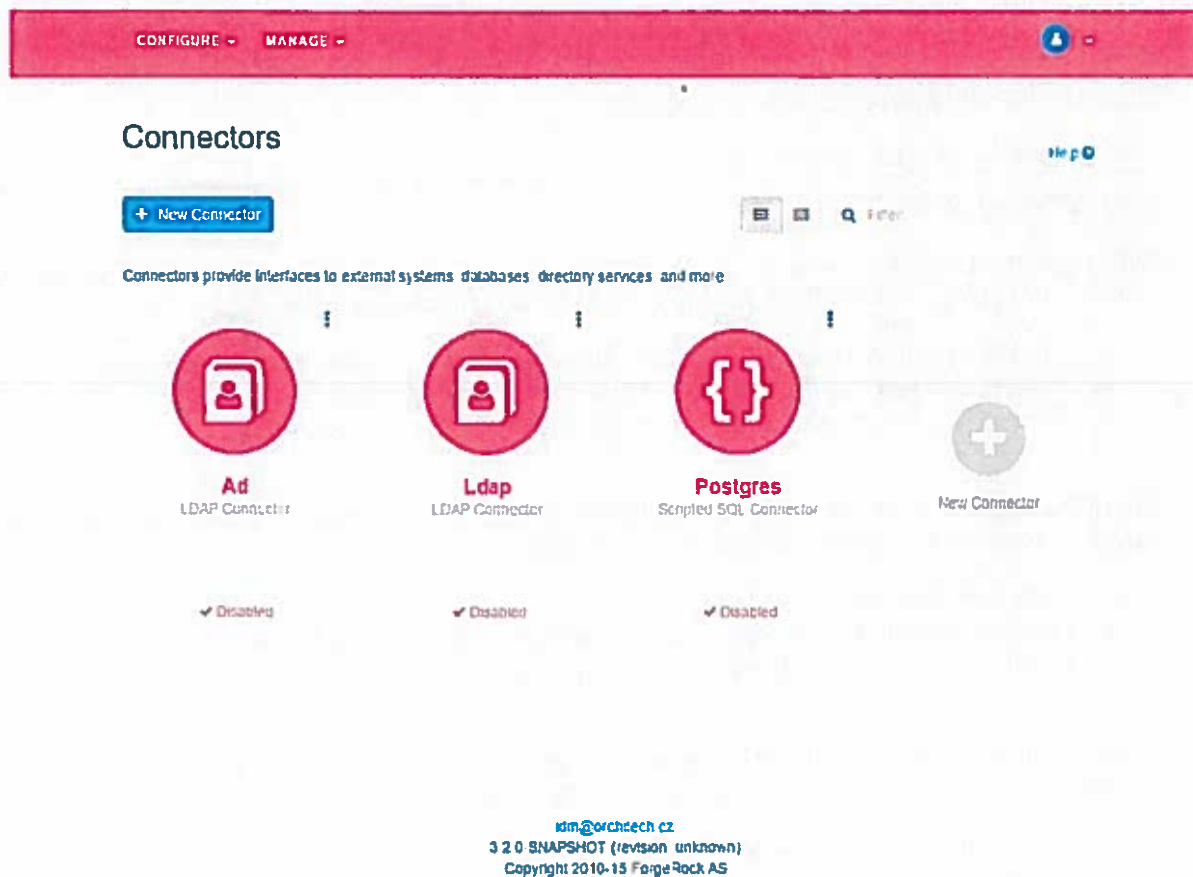
Součástí dodávaného řešení je nadstavba obsahující pokročilé uživatelské rozhraní s funkcionalitami pro privilegované uživatele (vizte vyjádření k požadavku kapitoly 5.1.3), tak rozhraní pro koncové neprivilegované uživatele (tzv. self-service rozhraní).

V rámci self-service je možné zobrazit stručné informace o vlastní identitě, vyžádat změnu hesla anebo požádat o přiřazení role.

Schvalovatelé v rámci uživatelského rozhraní vidí seznam požadavků čekajících na jejich vyjádření. Z rozhraní je pak možné požadavky schválit nebo zamítnout. Ve vlastní sekci je pak dostupný seznam historických zadaných a nebo schválených/zamítnutých žádostí. Přehled podřízených uživatelů pro nadřízené pracovníky je dostupný ve více kontextech, může být i na domovské stránce.

Práva pro jednotlivé sekce uživatelského rozhraní se řídí přiřazením interních rolí a lze je samozřejmě nastavit dle požadavku.

Více informací k technologiím a kompatibilitě uživatelského rozhraní je uvedeno ve vyjádření k požadavkům z kapitoly 5.1.3.



Obr. 2: Příklad obrazovky "seznam konektorů" (ukázka anglické mutace)



> Seznam uživatelů

Search

U.D	Uživatelské jméno ↑	Křestní jméno	Příjmení
1	msed	Martin	Sedlák
2	vhak	Vlasta	Hák
3	pjandova	Petra	Jandová
4	jstříh	Jindřich	Střih
5	mcrech	Marián	Ořech
6	hpavlova	Hanna	Pavlová
7	hstara	Helena	Stará
8	zdrboutova	Zora	Drboutová
9	esedma	Eva	Sedmá
10	hermanova	Lida	Hermanová

Zařazení na stránku 10 1 - 10 z 59

Obr. 3: Obrazovka s přehledem uživatelů

UID	3
Externí ID	Jandova_Petra_3
Zaměstnanecké ID	11185
Studentské ID	-
Uživatelské jméno	pjandova
Heslo
FreeRADIUS heslo
Interní role	-
Globální zámek	Odemčeno
Zámek FreeRADIUS	Odemčeno
Křestní jméno	Petra
Příjmení	Jandová
Rodné číslo	385212087
Korporátní email	-

Business Logic Orch.tech Solutions

Obr. 4: Příklad obrazovky "profil uživatele" v uživatelském rozhraní

1.2.4 Řízení hesel (5.2.4)

Požadavek zadavatele:

IDM systém umožňuje definovat různé politiky hesel, které určují složitost hesla. Tyto politiky hesel lze přiřazovat jednotlivým řízeným systémům nebo samotnému IDM systému, takže jsou při změně hesel z IDM rozhraní aktivně vynucovány.

OpenIDM zahrnuje konfigurovatelný *policy engine*, který umožňuje definovat komplexní politiky na jednotlivé atributy (nebo celé objekty) spravovaných objektů. Heslová politika je

jednou z takovýchto validací. V případě komplexních pravidel je možné politiky naskriptovat. Objekty, na něž jsou politiky vázány, pak není možné uložit, pokud dané politiky nesplňují.

EN CS mixed

Změna uživatelského hesla

Současné uživatelské heslo
.....

Validní uživatelské heslo:

- Obsahuje alespoň 3 skupiny znaků z těchto čtyř: velká písmena, malá písmena, číslice a speciální znaky (,;:! etc.).
- Neobsahuje jméno, příjmení nebo už. jméno uživatele.
- Obsahuje alespoň 8 znaků.
- Neobsahuje mezery.

Nové uživatelské heslo
.....

Heslo musí splňovat požadavky na sílu hesla.

Potvrzení nového hesla

ZMĚNIT HESLO ZRUŠIT

Business Logic | Onitech Solutions

Obr. 5: Obrazovka „změna hesla“

1.2.5 Manuální správa IDM uživatelů (5.2.5)

Požadavek zadavatele:

IDM systém nabízí možnost správy IDM uživatelů, kteří nejsou importováni z HR systému. Jedná se o skupinu uživatelů (např. externisté), kteří jsou do IDM systému zakládáni ručně IDM operátorem. Veškerá obsluha je prováděna z webového uživatelského rozhraní, v kterém je umožněno provádět následující akce:

- Založení IDM uživatele
- Aktualizace IDM uživatele
- Deaktivace/Aktivace IDM uživatele

Tito uživatelé nejsou nijak ovlivněni HR importem.

Založení, aktualizace a aktivace/deaktivace IDM uživatelů jsou funkce webového uživatelského rozhraní.

Uživatelé bez vazby na HR import jsou standardními uživateli s tím rozdílem, že nemají definován vazbu na HR (tzv. link). V rámci uživatelského rozhraní je možné nadefinovat, které uživatele je možné modifikovat, případně které atributy je možné modifikovat. Je možné nadefinovat, aby uživatelům z HR bylo možné upravovat několik vybraných atributů, kdežto u uživatelů bez vazby na HR půjde editovat všechny atributy.

Aktivace a deaktivace uživatelů bez vazby na HR využije stejný mechanismus aktivace / deaktivace, který existuje pro standardní uživatele s vazbou na HR.

1.2.6 Reconsiliace (5.2.6)

Požadavek zadavatele:

System podporuje tzv. reconsiliaci řízených systému, tedy proces, v rámci kterého jsou porovnány skutečné účty s jejich předpokládaným obrazem vypočteným IDM systémem. Výsledkem je buď automatická akce v podobě opravy, nebo notifikace.

V rámci tohoto procesu jsou také identifikovány účty na řízeném systému, které nemají svůj protějšek v IDM systému.

OpenIDM podporuje plnou reconciliaci objektů mezi zdrojovým a cílovým systémem. Detekované rozdíly OpenIDM kategorizuje dle tzv. *synchronizačních situací*, např.:

- objekt existuje jen ve zdrojovém systému
- objekt existuje jen v cílovém systému
- objekt existuje v obou systémech, ale má odlišné atributy
- objekt existuje

Pro jednotlivé synchronizační situace je možné definovat konkrétní akce, které má OpenIDM vykonat:

- založení / smazání / update objektu v cílovém systému
- vytvoření / zrušení vazebního objektu (linku) mezi objekty
- vyvolání výjimky
- zalogování situace (případně odeslání notifikace)
- ignorování situace

System tedy umožňuje detekovat a reagovat na nepovolené účty a tzv. sirotky (orphan accounts).

1.2.7 Dávkové operace (5.2.7)

Požadavek zadavatele:

System poskytuje rozhraní pro dávkový import/export IDM objektů (uživatel, účet, role, oprávnění, vazby mezi objekty, ...).

System podporuje import / export IDM objektů ve formátu CSV.

1.3 Platformy – návrh technologií a nasazení řešení

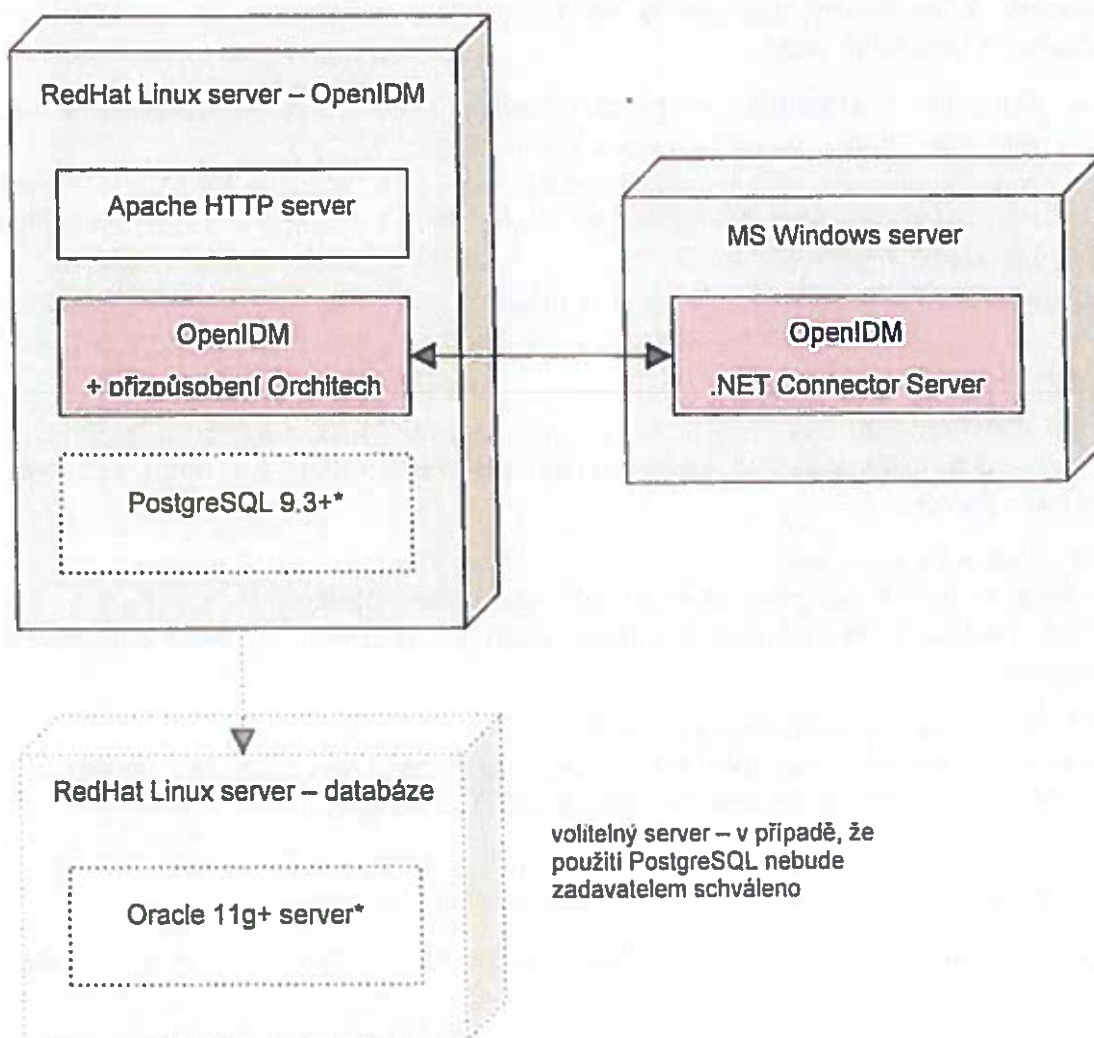
Systém OpenIDM spolu s přizpůsobením a konfigurací Orchitech jsou navrženy tak, aby spolupracovaly s celou řadou platforem, operačních systémů, databázových systémů i webových prohlížečů.

Mezi podporované platformy patří oba zadavatelem preferované systémy – jak RedHat Enterprise Linux verze 6 a vyšší (64 bit), tak Windows Server 2012 R2 a vyšší. Obecným požadavkem je funkční Java Virtual Machine (JDK) verze 1.7 nebo novější.

Mezi podporované databázové systémy patří:

- PostgreSQL verze 9.3 a vyšší (za určitých okolností je možné jej považovat za součást OS RedHat Enterprise Linux verze 6 a vyššího)
- Oracle 11g a vyšší
- Microsoft SQL server verze 2008 a vyšší
- MySQL verze 5.1 a vyšší

Uchazeč navrhuje uspořádání serverů dle obrázku níže.



Obr. 6: Nasazení komponent mezi servery

RedHat Linux server – OpenIDM poběží na zadavatelem preferovaném RedHat Enterprise Linux AS. Na tomto serveru poběží většina komponent systému včetně:

- Apache HTTP serveru, který bude „vstupní branou“ většiny administrátorských přístupů (v této fázi projektu) a požadavků běžných uživatelů (v dalších fázích projektu),
- OpenIDM + přizpůsobení Orchitech; včetně konektorů (kromě MS Windows konektorů),
- PostgreSQL 9.3+ – uchazečem preferovaný databázový stroj, lze k němu přistupovat jako k součásti OS. Tento lze v případě nutnosti nahradit podporovanou databází dle preference zadavatele běžící na jiném serveru – ať již sdílenou nebo dedikovanou.

MS Windows server – je server, na němž jsou provozovány konektory specifické pro prostředí Microsoft, jde o konektory založené na Windows PowerShell (zejména MS Exchange).

Redhat Linux server – databáze je zde naznačen jen pro úplnost pro případ, že by zadavatel trval na použití databáze Oracle.

Vzhledem k flexibilitě nabízeného řešení je řada možností, jak vycházet vstříc preferencím zákazníků, např.:

- Nepoužití PostgreSQL na serveru RedHat Linux server – OpenIDM a využití databáze Oracle, jak je naznačeno v textu výše.
- Navíc k možnosti výše je možné nasadit vše v rámci jednoho MS Windows serveru (pro každé prostředí). Nicméně výše navržená varianta lépe odpovídá zadavatelem preferovaným platformám.

Tato flexibilita rovněž zajišťuje, že nebude problém splnit příslušné interní směrnice MZe, mj. směrnici „Definice závazné architektury a požadavků pro vývoj a zabezpečení provozu registrů a klíčových aplikací MZe“.

Není-li v dokumentu uvedeno jinak, rozumí se jako výchozí varianta Redhat Linux server – OpenIDM s databázovým systémem PostgreSQL 9.3 nebo vyšší a MS Windows server.

1.3.1 Testovací prostředí

Testovací prostředí uchazeč navrhuje jako identické s produkčním prostředím. Bude-li zvolena některá z nastíněných alternativ, testovací prostředí by mělo být provedeno analogicky.

1.3.2 Specifikace požadovaných serverů

Řešení a jeho navržené nasazení dle obrázku 6 je možné provozovat jako virtuální servery na virtualizační platformě zadavatele (VMWare ESX 5.0 a vyšší).

Pro uchazečem preferovanou variantu s použitím PostgreSQL verze 9.3 nebo vyšší uchazeč specifikuje 2 virtuální servery s následujícími parametry:

- **Redhat Linux server – OpenIDM:** 2 jádra, 40 GB disk, 4 GB RAM, OS RedHat Enterprise Linux verze 6 a vyšší
- **MS Windows:** 1 jádro, 40 GB disk, 4 GB RAM, OS MS Windows 2012

Pro testovací prostředí by pak šlo o téměř stejné virtuální servery:

- **Redhat Linux server – OpenIDM:** 1 jádro, 40 GB disk, 4 GB RAM, OS RedHat Enterprise Linux verze 6 a vyšší
- **MS Windows:** 1 jádro, 40 GB disk, 4 GB RAM, OS MS Windows 2012

Výše uvedené parametry zcela postačují na počty uživatelů uvedené v části 5.3.1 technické specifikace, včetně množství účtů, které lze na základě uvedených informací předpokládat.

1.3.3 Specifikace požadavků na parametry komunikačních tras a síťových přístupů mezi jednotlivými komponentami IDM systému

Pro definici přístupů jsou použita následující označení:

- Komponenty IDM (analogicky k předchozí kapitole)
 - OpenIDM – Redhat
 - OpenIDM – Windows
- Integrované systémy
 - AD
 - Exchange
 - SAP CUA
 - SAP HR

Odkud	Kam	Port	Popis
OpenIDM – RedHat	OpenIDM – Windows	8759	Konektivita OpenIDM na .NET Connector Server
* (intranet)	OpenIDM – Redhat	443 (HTTPS)	Přístup na uživatelské rozhraní.
OpenIDM – Windows	Exchange	5985, 5986	Konektivita OpenIDM na Exchange server.
OpenIDM – RedHat	AD	389, 636	Konektivita OpenIDM na AD.
OpenIDM – RedHat	SAP CUA	32xx	Konektivita OpenIDM na SAP CUA.
OpenIDM – RedHat	sdílený disk	porty potřebné pro SMB/CIFS, resp. dle technologie sdíleného disku	Stahování CSV exportu HR dat
Administrátoři OS a OpenIDM	správa serverů	22, 3389	vzdálená plocha / SSH
Systém SIEM	OpenIDM – RedHat	dle metody čtení auditních záznamů (5432 pro	Integrace OpenIDM se systémem SIEM.

		JDBC konektor)	
--	--	-------------------	--

1.3.4 Seznam dodaných licencí

- OpenIDM a jeho komponenty: open-source licence (Common Development and Distribution License – CDDL)
- Přizpůsobení Orchitech: neomezená nevýhradní licence včetně práva vytvářet odvozená díla
- PostgreSQL (bude-li nasazena a nebude-li považována za součást OS): open-source licence (PostgreSQL License)
- OpenJDK (Java pro Linux) – součást OS Redhat Enterprise Linux
- Oracle Java SE Development Kit pro MS Windows – Oracle Binary Code License Agreement for Java SE

Uchazeč prohlašuje, že všechny komponenty řešení jsou v souladu s licenčními požadavky zadavatele tak, jak jsou definovány v zadávací dokumentaci. Licence nejsou omezeny počtem uživatelů.

PŘÍLOHA Č. 2

SPECIFIKACE KATALOGOVÝCH LISTŮ



MINISTERSTVO ZEMĚDĚLSTVÍ

Specifikace katalogových listů

Poskytnutí IDM řešení

OBSAH

1. Přehled základních pojmů.....	39
2. Podmínky poskytování služeb Systému.....	40
2.1. Obecné podmínky	40
2.2. Dokumentace.....	41
2.2.1. Provozní deník.....	41
2.3. Změny v Systému provedené Objednatelem.....	42
3. Sleva z ceny a smluvní pokuty.....	42
3.1. Uplatnění slevy z ceny služeb a možnost odstoupení od Smlouvy.....	43
4. Vyhodnocování kvality poskytovaných služeb.....	43
4.1. Měření Služeb.....	43
4.2. Kategorie provozních stavů	43
4.3. Stanovení priorit incidentů a požadavků a jejich SLA.....	43
4.3.1. Priority pro provozní prostředí.....	43
5. Seznam katalogových listů	45
5.1. IDM01 Odezva.....	45
5.2. IDM02 Maintenance.....	46
5.3. IDM03 Správa IDM systému.....	48
5.4. IDM04 Reparametrizace a optimalizace.....	50

1. Přehled základních pojmů

Termín	Význam
Celková měsíční cena	Součet paušálních měsíčních cen za katalogové listy, u kterých je placena paušální měsíční cena
Člověkoden	Představuje 8 hodin práce jednoho pracovníka
Helpdesk	Specializované oddělení zajišťující komplexně uživatelskou podporu
Check-out/check-in hesla	funkce umožňující získání (check-out) hesla ke spravovanému privilegovanému účtu na základě oprávnění uživatele (a následné oznámení o konci jeho využití – check-in)
IDM	Identity Management – správa uživatelských účtů
ITSM	IT service management – řízení úrovně poskytovaných Služeb především, nikoliv však výhradně, v rozsahu doporučeném ITIL
KL	katalogový list
KPI	výkonnostní parametr, hodnotící parametr Služby
Maintenance	Služby a aktivity, poskytované výrobcem Systému nebo jeho komponent, potřebné pro udržení Systému v provozuschopném stavu v souladu s dohodnutými parametry a zajišťující kompatibilitu Systému s komponentami ICT Objednatele.
MZe	Česká republika - Ministerstvo zemědělství
Objednatel, Zadavatel	osoba, která je jako Objednatel definovaná v záhlaví Smlouvy
Obnovení služby (fix time)	Je časová lhůta, ve které je Zhotovitel povinen obnovit parametry Služby, resp. Systému, na sjednanou úroveň s tím, že doba obnovení parametrů Služby, resp. Systému, je počítána od vzniku původního požadavku bez ohledu na změnu priority požadavku
Odezva (response time)	Je časová lhůta, ve které je Zhotovitel povinen odpovědět na požadavek předaný prostřednictvím Service Desku Objednatele, a to buď odmítnutím, nebo přijetím požadavku
Pracovní den	každý den mimo sobotu, neděl a státních svátků a ostatních svátků dle zákona č. 245/2000 Sb., o státních svátcích, o významných dnech a o dnech pracovního klidu, ve znění pozdějších právních předpisů
Pracovní doba nebo Kalendář	doba, kdy je Služba poskytována – od-do, které dny v týdnu, počet minut pro potřeby výpočtu dostupnosti: 8x5 - Pracovní dny od 8:00 do 16:00
Provozní deník	dokumentace obsahující náležitosti uvedené v kapitole 2.2.1 této přílohy č. 2 Smlouvy
Rozhraní Systému	integrační a komunikační rozhraní Systému prezentované vnějším rozhraním hraničního (posledního) aktivního síťového prvku pod správou Zhotovitele, tvořícího rozhraní mezi sítí Zhotovitele a vnější komunikační infrastrukturou
Service Desk (SD)	Nástroj pro podporu řízení služeb
Servisní okno	časový interval definovaný Objednatelem a zakotvený v dokumentaci MZe
SLA	sjednaná úroveň poskytované Služby
Služba	služba Podpory definovaná v jednotlivých KL
Smlouva	Smlouva o poskytnutí řešení „Poskytnutí IDM řešení“ uzavřená mezi Objednatelem a Zhotovitelem
SSO (Single-Sign-On)	systém jednotného přihlášení umožňující autentizaci do dalších systémů na základě jednoho přihlášení bez nutnosti dalšího zadávání přístupových údajů

SW	software, aplikace – program, programové vybavení nebo jeho komponenta
Standardní SW (SSW)	softwarové vybavení třetích stran dodané v rámci Smlouvy, na základě kterého byl zhotoven Systém, které nebylo vyvinuto Zhotovitelem a není aplikační SW komponentou Systému vyvinutou v rámci Smlouvy
Systém	IDM systém, předmět dodávky
Výrobce	Subjekt, který pro daný produkt zastřešuje vývoj a údržbu, tedy zejména opravy chyb, testování nových verzí
Zhotovitel	osoba, která je jako Zhotovitel definovaná v záhlaví Smlouvy

2. Podmínky poskytování služeb Systému

2.1. Obecné podmínky

Zhotovitel je povinen bezplatně poskytnout součinnost pro MZe související s odbornými, zákonnými a jinými kontrolami a audity, které mohou být uplatňovány vůči MZe v souvislosti s dodávkou služeb a Systémem jako takovým.

Veškeré výkazy, podklady a dokumenty musí být ve formě, umožňující přezkoumatelnost a auditovatelnost ze strany kontrolních organizací, kterými se rozumí veškeré subjekty oprávněné provádět kontrolu jakkoliv týkající se plnění této Smlouvy na základě právního předpisu. Pokud je dokument, výkaz nebo jiný podklad, související s tímto dokumentem zpochybněn kontrolní organizací, je Zhotovitel povinen poskytnout podklady, které budou kontrolním orgánem akceptovány. V případě, že Zhotovitel nebude schopen tyto podklady dodat a/nebo tyto nebudou kontrolním orgánem akceptovány a pokud absence těchto dokumentů bude důvodem k udělení sankce vůči MZe, Zhotovitel poskytne náhradu ve výši sankce, uplatněné vůči MZe, a to i po uplynutí účinnosti této Smlouvy, pokud se sankce bude týkat období trvání Smlouvy.

Zhotovitel je před zahájením dodávky Služby Objednateli povinen dodat písemný seznam komponent Systému, které kategorizuje jako standardní software, krabicový software případně software třetích stran a takto označit i odpovídající položky konfigurační databáze Objednatele.

Všechny úpravy, funkcionality, programové kódy, konfigurace apod., které Zhotovitel neoznačí jako standardní software a/nebo které vznikly v průběhu platnosti Smlouvy, jsou považovány za vlastnost Systému, kterou může Objednatel kdykoliv na základě vlastního uvážení využít v jiných informačních systémech a libovolně upravovat bez jakýchkoliv licenčních závazků vůči Zhotoviteli nebo třetím stranám. Tím nejsou dotčena práva Objednatele ani povinnosti Zhotovitele dle Smlouvy.

Pokud je zjištěno podávání nepravdivých dat a výkazů Zhotovitelem, je celé měřicí období, ve kterém bylo toto zjištěno, považováno za nesplněné ve všech parametrech, u kterých bylo toto pochybení zjištěno. Vyplyvající slevy jsou aplikovány na každý parametr zvlášť v maximálním rozsahu stanoveném touto Smlouvou.

Zhotovitel je povinen se řídit zákonnými, technickými a jinými požadavky, pravidly a doporučeními, souvisejícími se zajišťovanými službami, spravovanou nebo využívanou infrastrukturou a využívanými nebo poskytovanými službami, které nejsou předmětem tohoto dokumentu.

Ústní jednání v souvislosti s předmětem dodávky / plnění definovaným Smlouvou nemá povahu jakéhokoliv závazku.

2.2. Dokumentace

Veškerá infrastruktura, která je předmětem dodávky Služeb, bude dokumentována. Zhotovitel zajistí aktualizaci při každé změně, provedené Zhotovitelem. Pokud dokumentace neexistuje, Zhotovitel ji v potřebném rozsahu vytvoří. Dokumenty dokumentace mají v úvodní sekci seznam změn, ve kterém jsou stručně shrnuty změny provedené od předchozího vydání dokumentace. Dokumentace zahrnuje zejména, nikoliv však výhradně následující položky:

- hlavní komponenty IDM systému na úrovni celků, na které lze aplikovat změnu ve smyslu doporučení ITIL;
- veškeré licence včetně volně šiřitelných a neplacených licencí;
- vazby mezi komponentami IDM systému na úrovni fyzické, logické, datové, dodávky služeb;
- uživatelskou dokumentaci;
- bezpečnostní dokumentaci;
- administrátorskou dokumentaci;
- zálohovací plány a postupy;
- opatření a dokumentace k zajištění kontinuity provozu (vč. plánů obnovy IDM systému);
- postupy pro obnovení dat včetně konfigurací do původního provozního stavu;
- konfigurace aplikací a případně jejich komponent;
- seznamy použitých softwarových komponent a standardního SW včetně jejich verzí;
- všechny programové kódy, vzniklé jako předmět dodávky, kromě Standardního SW;
- všechny programové kódy, vzniklé nebo změněné v průběhu platnosti Smlouvy;
- konfigurace a artefakty, nezbytné pro sestavení programových komponent z programových kódů;
- Provozní deník;

2.2.1. Provozní deník

Zhotovitel je povinen při poskytování Služeb dle této Smlouvy vést Provozní deník. Provozní deník bude veden jeden pro celý Systém.

Zhotovitel je povinen do Provozního deníku prostřednictvím záznamu zaznamenat minimálně následující události a to nejdéle do 4 hodin od provedení změny:

- Provedení úkonů předepsaných v KL včetně identifikace příslušného KL;
- Havarijní stavy, opravy, výměny komponent;
- Anomálie a nestandardní stavy systémů, které mají dopad na plnění SLA;
- Zprovoznění nového nebo dočasně odstaveného systému a/nebo odstavení systému;
- Spuštění, vypnutí a restart systému;
- Obnovení ze zálohy.

Každý záznam bude obsahovat minimálně následující informace:

- Datum a čas pořízení záznamu;
- Identifikace osoby pořizující záznam;
- V případě události trvajících více než 1 hodinu také čas začátku a konce události,

- Popis události.
- Provedené úkony k události s uvedenými časy provedení
- Zdůvodnění, na základě jakého požadavku byla činnost vykonána (např. ID záznamu v Service Desku Objednatele, číslo Smlouvy a příslušný KL).

Pro vyloučení pochybností se uvádí, že Provozní deník není systémovou dokumentací. Při realizaci změny se do Provozního deníku zapisuje, že byla provedena změna a její stručný popis. Popis změny, resp. nově vzniklý stav a konfigurace systému jsou detailně popisovány v systémové dokumentaci. Pro vyloučení pochybností se uvádí, že změnou se myslí jakákoliv změna ve smyslu „Change management“ podle ITIL.

Způsob vedení Provozního deníku není předepsán. Zhotovitel je oprávněn vést Provozní deník v elektronické podobě, avšak tak, aby byl pro Objednatele a jeho pracovníky kdykoliv přístupný a bylo možno z něj provádět kopie, přehledy a exporty dat.

Objednatel připouští vedení jednotného Provozního deníku pro všechny KL. V takovém případě každý záznam obsahuje také identifikaci KL, ke kterému se vztahuje.

2.3. Změny v Systému provedené Objednatelem

Objednatel je oprávněn provádět změny (administrovat) v Systému pomocí standardního rozhraní Systému (např. přidávat/odebírat uživatele, přidávat/odebírat notifikace, zálohovat Systém, apod.) do míry, na kterou je Systém Zhotovitelem naddimenzován na základě informací uvedených v Technické specifikaci. Tyto změny nijak neovlivní povinnosti Zhotovitele dané katalogovými listy.

V případě jiných změn (např. úprava konfigurace konektoru na řízený systém) realizovaných za účinnosti Smlouvy je Objednatel povinen nechat si takovou změnu schválit Zhotovitelem, který tak vyhodnotí dopady na funkčnost Systému. V případě neakceptace změny Zhotovitelem, musí zhotovitel navrhnout jiné řešení, které bude mít na Systém stejný účinek. Provedení změn Objednavatelem podle postupu schváleného Zadavatelem nezbavuje Zhotovitele povinností ze zajištění parametrů služeb definovaných v KL.

3. Sleva z ceny a smluvní pokuty

Slevy z ceny za nedodržení celkové dostupnosti a za nedodržení Obnovy služby vzniklé v souvislosti se stejným incidentem lze kumulovat.

Zhotovitel není v prodlení s plněním povinností, na jejíž porušení se sleva z ceny nebo smluvní pokuta vztahuje, a to po dobu, pro kterou prokáže, že za porušení povinností Zhotovitel neodpovídá (např. prokázána příčina ležící mimo Systém).

Uplatnění slevy nebo smluvní pokuty nemá vliv na povinnost poskytování Služeb ve sjednaných úrovních. Nárok na slevu z ceny Služeb nebo smluvní pokutu se nedotýká závazku Zhotovitele splnit povinnost, se kterou je v prodlení (pokud je to vzhledem k povaze předmětné Služby objektivně možné).

Objednatel má právo v případě porušení parametrů definovaných katalogovými listy na slevy z ceny nebo na smluvní pokuty ve výši stanovené v jednotlivých katalogových listech.

3.1. Uplatnění slevy z ceny služeb a možnost odstoupení od Smlouvy

Součet všech poskytnutých slev z ceny Služeb v daném měsíci se odečte od Celkové měsíční ceny všech poskytnutých Služeb za daný měsíc. Objednatel má za daný měsíc nárok na zaplacení ceny za poskytnuté Služby pouze ve výši takto vypočteného rozdílu.

V případě, že součet všech poskytnutých slev z ceny poskytnutých Služeb v daném měsíci je vyšší než Celková měsíční cena poskytnutých Služeb za daný měsíc, bude neuplatněn nárok na slevu z ceny Služeb uplatněn v dalším měsíci.

V případě, že výše neuplatněné slevy z ceny Služeb převyší součet cen Služeb za následující měsíce až do konce trvání Smlouvy, je Objednatel oprávněn od Smlouvy odstoupit. Objednatel je současně oprávněn před odstoupením od Smlouvy vyúčtovat Zhotoviteli částku odpovídající výši neuplatněné slevy z ceny Služeb jako smluvní pokutu.

Odstoupení od smlouvy nemá vliv na výši uplatněné slevy ani smluvní pokutu.

4. Vyhodnocování kvality poskytovaných služeb

4.1. Měření Služeb

Objednatel bude provádět dostupnými prostředky kontrolu provádění činnosti dle katalogového listu. Pokud Objednatel identifikuje, že dotčená činnost nebyla vykonána nebo byla vykonána v rozporu s požadavky vyplývajícími ze Smlouvy, zaznamená tuto skutečnost do Service Desku Objednatele prostřednictvím přidělení incidentu Zhotoviteli.

4.2. Kategorie provozních stavů

Jsou definované následující kategorie provozních stavů:

Standardní provoz

Provoz na provozním nebo testovacím prostředí je bez omezení, Systém je plně funkční.

Servisní okno

Objednatelem předem definovaný a oznámený časový interval na provozním nebo testovacím prostředí, ve kterém může dojít ke snížení nebo omezení funkčnosti Systému nebo některé z jeho částí. Po jeho dobu Objednatel neuplatňuje slevy z ceny. O vyhlášení Servisního okna rozhoduje MZe.

4.3. Stanovení priorit incidentů a požadavků a jejich SLA

Priority incidentů a požadavků stanovuje Objednatel.

4.3.1. Priority pro provozní prostředí

Je-li tak definováno v příslušných KL, platí priority uvedené níže. Pro definici priority požadavků dle KL IDM01 a IDM03 se uplatní pravidla uvedená v předmětném KL.

<i>Priorita</i>	<i>Definice priority požadavku</i>	<i>Parametry řešení požadavku</i>
Priorita 1 Kritická	Některé nebo všechny části IDM systému selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost IDM systému.	Odezva: 1 den Obnovení služby: 2 dny
Priorita 2 Vysoká	IDM systém je funkční pouze částečně, IDM systém je ovlivněn selháním nebo omezením některé z komponent nebo funkcí podporujících důležité činnosti IDM systému.	Odezva: 1 den Obnovení služby: 3 dny
Priorita 3 Střední	IDM systém je funkční, závada nemá vliv na činnost IDM systému. Vyskytují se nedostatky nepodstatné povahy, které způsobují například nekomfortnost obsluhy nebo zvyšující pracovní činnosti než v běžném provozu.	Odezva: 2 dny Obnovení služby: 5 dní
Priorita 4 Nízká	Bezpečnostní hrozba, která má dopad na IDM systém.	Odezva: 2 dny Obnovení služby: 5 dny
Priorita 5 Ostatní	Požadavkem je žádost o podání informace (dotaz, vysvětlení) nebo existence aktualizace či záplat Systému. Priorita požadavku zároveň zahrnuje situace, kdy některé funkce prokazatelně selhaly, ale nejsou v daný moment využívány nebo nemají žádný vliv na řádný chod Systému, za předpokladu, že řešení požadavku závisí na součinnosti třetí strany mimo vliv Zhotovitele.	Odezva: 3 dny Obnovení služby: 15 dnů

5. Seznam katalogových listů

5.1.IDM01 Odezva

Katalogový list Služby	
Identifikace (ID)	IDM01
Název Služby	Odezva
Popis Služby	Zajištění odezvy služeb, funkcí a dat IDM systému.
Parametry	
Název	KPI01 Odezva
Definice	Zajištění dostupnosti Služby <ul style="list-style-type: none"> Obnovení funkcí IDM systému či některé z jeho komponent podle priorit definovaných v 4.3.1 Priority pro provozní prostředí;
Parametry KPI	
Kalendář služby	8x5
Odezva	Viz 4.3.1 Priority pro provozní prostředí
Obnovení služby	Viz 4.3.1 Priority pro provozní prostředí
Definice parametrů	<p>Odezva Systému je definována následovně:</p> <ol style="list-style-type: none"> Je možné se úspěšně přihlásit do všech komponent Systému. <ul style="list-style-type: none"> Funkce přihlášení se do Systému se považuje za dostupnou, pokud se uživateli zobrazí kompletní uživatelské rozhraní Systému (dále jen „Odezva systému na přihlášení“) do 5 vteřin od potvrzení přihlašovacích údajů, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem; Pokud je Odezva Systému na přihlášení v intervalu od 5 do 10 vteřin, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, je tento stav považován jako závada Priority 3; Pokud je Odezva Systému na přihlášení delší než 10 vteřin, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, nebo pokud se není možné do Systému přihlásit, je tento stav považován jako závada Priority 1; Po přihlášení do Systému jsou uživatelé k dispozici všechny jemu přiřazené funkce/role/nástroje; <ul style="list-style-type: none"> Pokud má uživatel po úspěšném přihlášení k dispozici pouze některé nikoliv všechny jemu přiřazené funkce/role/nástroje, jedná se o závadu Priority 2; Pokud uživatel nemá po úspěšném přihlášení k dispozici žádné jemu přiřazené funkce/role/nástroje, jedná se o závadu Priority 1; Celková délka trvání importu uživatelů z HR systému netrvá déle než 8 vteřin na uživatele (počítáno jako průměr). Doba je měřena od úspěšného načtení uživatele z HR systému po počátek volání instrukce na založení/změnu účtu v řízeném systému; <ul style="list-style-type: none"> Pokud délka trvání importu (průměr na uživatele) je v intervalu od 8 do 14 vteřin, jedná se o závadu Priority 2; Pokud délka trvání importu (průměr na uživatele) trvá déle než 14 vteřin, jedná se o závadu Priority 1; Systém audituje jak veškeré operace uživatelů/administrátorů v rámci Systému, tak i interní operace Systému samotného; <ul style="list-style-type: none"> Funkce auditování operací se považuje za dostupnou, pokud je auditní záznam o operaci v Systému zaznamenán a zároveň dostupný ke kontrole do 5 vteřin po provedení příslušné činnosti, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem; V opačném případě se jedná o závadu Priority 3; Systém odesílá notifikace dle konfigurace;

	<ul style="list-style-type: none"> Funkce odesílání notifikací se považuje za dostupnou, pokud mají notifikace správný obsah a odesílají se do 10 vteřin od události, na které je notifikace konfigurována. Výjimku tvoří druhý a další výskyt stejné události v krátkém sledu za sebou, který může způsobit zahlcení; V opačném případě se jedná o závadu Priority 3; <p>Je-li v tomto katalogovém listu uvedeno, že se jedná o závadu určité priority, aplikují se pro dané priority příslušné doby odezvy a obnovení služby požadavků dle Parametrů řešení požadavku ve smyslu článku 4.3.1 Priority pro provozní prostředí.</p>
Způsob výpočtu a měření	Jako směrodatné a závazné pro Zhotovitele se pro měření uvedených parametrů odezvy Systému berou hodnoty naměřené dohledovým systémem Objednatele. V případné zjištění nedostupnosti, nefunkčnosti či omezení funkce Systému je tento stav zaznamenán do Service Desku Objednatele. Pracovníci Helpdesku Objednatele následně kontaktují kanálem, definovaným Smlouvou (email, telefon, Service Desk Objednatele), technickou podporu Zhotovitele a o tomto kontaktování provedou záznam do tiketu v Service Desku Objednatele jako počátek nedostupnosti Služby.
Měřicí bod	Service Desk Objednatele.
Způsob dokladování	Měsíční report o plnění KPI.
Sleva z ceny	Jednorázová sleva z ceny ve výši 10.000,- Kč bez DPH v případě porušení dohodnuté doby pro Obnovení služby viz tabulka Priorit v kapitole viz 4.3.1 Priority pro provozní prostředí a zároveň další sleva z ceny ve výši 1000 Kč za každou započatou hodinu nad dohodnutou dobu pro Obnovení služby viz tabulka Priorit v kapitole 4.3.1 Priority pro provozní prostředí.
Doplňující informace	
Poznámka	-
Platební podmínky	Paušální měsíční cena podle Smlouvy.

5.2. IDM02 Maintenance

Parametry ID Služby	
Identifikace (ID)	IDM02
Název Služby	Maintenance
Popis Služby	Technická podpora produktu
Parametry	
Název	KPI02 Maintenance
Definice	Zajištění technické podpory směrem k výrobcí dané nárokem platné Maintenance na komponenty IDM systému.
Parametry KPI	
Kalendář služby	8x5
Odezva	Podle Priority 3
Obnovení služby	Podle Priority 3
Definice parametrů	<p>Přímý přístup Objednatele a Zhotovitelem zprostředkovaný přístup ke službám, souvisejících s Maintenance, všech výrobců všech komponent Systému. Jedná se zejména, nikoli však výhradně, o tyto služby:</p> <ul style="list-style-type: none"> přístup a možnost využití kontaktního místa podpory výrobce možnost zadávat požadavky, související se zajištěním provozuschopnosti a aktualizacemi Systému možnost získávání všech typů aktualizací a opravených verzí přístup do znalostní báze daného výrobce užívání všech výhod a služeb, které výrobce v rámci Zhotovitelem poskytnutého typu Maintenance poskytuje

	<ul style="list-style-type: none"> • zajištění všech informací a součinností, vyžadovaných výrobcem v souvislosti s poskytováním Maintenance a podpory <p>Tyto služby jsou hrazeny tímto KL a Objednateli nevznikne uplatněním požadavku u výrobce v rámci KL IDM02 žádný dodatečný náklad.</p> <p>Veškeré podklady související se zajištěním Maintenance (licence, přístupové údaje na portály výrobců, kontaktní údaje na kontaktní místa výrobce – email, telefon, apod.) budou předány Objednateli a Zhotovitel bude zajišťovat jejich aktuálnost směrem k Objednateli po celou dobu účinnosti Smlouvy.</p>
Způsob výpočtu a měření	<p>Kontrola dostupnosti služeb výrobců, souvisejících s KL IDM02. Počátkem nedostupnosti je čas záznamu v Service Desku Objednatele, kterým oznamuje Zhotovitel nedostupnost služeb pro každou Maintenance pro každou komponentu Systému.</p> <p>Doklady, prokazující platnost Maintenance a podpory na vyžádání a/nebo při změně (vč. obnovení) smluv s výrobcem. Nesmí dojít k nezajištění Maintenance a podpory.</p>
Měřicí bod	Service Desk Objednatele.
Způsob dokladování	Záznam v Service Desku Objednatele.
Smluvní pokuta	Objednatel má právo na uhrazení smluvní pokuty ve výši 5.000,- Kč za každý případ porušení povinnosti Zhotovitele zajistit Maintenance v souladu s tímto katalogovým listem v daném měsíci (tzn. Maintenance nebude zajištěna vůbec nebo bude zajištěna v rozporu se sjednanými parametry). Objednatel má dále právo na smluvní pokutu 5.000,- Kč za každý případ porušení parametru Obnovení služby pro kteroukoliv z činností definovaných výše v rámci Definice parametrů.
Definice parametrů	
Poznámka	Doba poskytování služby Maintenance je určena ve Smlouvě.
Platební podmínky	Jednorázová platba za Maintenance produktu/produktů IDM systému.

IDM03 Správa IDM systému

Katalogový list Služby	
Identifikace (ID)	IDM03
Název Služby	Správa IDM systému.
Popis Služby	Zajištění správy všech komponent dodaného IDM systému.
Parametry	
Název	KPI03 Správa IDM
Definice	<p>Správa IDM systému zahrnuje především, nikoliv však výhradně, následující činnosti:</p> <ul style="list-style-type: none"> • Provoz a správa všech komponent IDM systému (SW, DB, OS), kromě operačního systému, pokud se jedná o MS Windows Server, nebo Red Hat linux poskytnutý Objednatelem. • Profylaktické činnosti • Kontrola výkonnosti IDM systému a návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře IS MZe • Identifikace aktualizací relevantních k prostředí Objednatele, ověření jejich dopadů v prostředí Objednatele a jejich aplikace na Systém Objednatele; • Aplikace schválených aktualizací na Systém • Posouzení dopadu nových aplikací požadovaných k instalaci na přístupové servery pro zajištění správy technologií v prostředí MZe
Parametry KPI	
Kalendář Služby	8x5
Odezva	Viz 4.3.1 Priority pro provozní prostředí
Obnovení služby	Viz 4.3.1 Priority pro provozní prostředí
Definice parametrů	<ul style="list-style-type: none"> • Sledování, identifikace, posouzení dopadů, poskytnutí stanoviska k nasazení a aplikace bezpečnostních aktualizací na Systému. Bezpečnostní aktualizace je aktualizace uvolněná výrobcem řešení pro produkční nasazení, která řeší bezpečnostní slabinu či zranitelnost řešení, zde se jedná o požadavek Priority 4; • Sledování, identifikace, posouzení dopadů, poskytnutí stanoviska k nasazení a aplikace aktualizací či záplat Systému. Zde se jedná o požadavek Priority 5. • Posouzení dopadu nových aplikací požadovaných k instalaci na přístupové servery pro zajištění správy technologií v prostředí MZe dle Priority 4 (viz 2.3 Změny v Systému provedené Objednatelem)
Způsob výpočtu a měření	<p>V případě vydání nové aktualizace/opravného balíku/nové verze SW výrobcem založí Zhotovitel požadavek do Service Desku Objednatele informující o této skutečnosti. Zhotovitel je povinen požadavek založit nejdříve do doby dané jako Odezva pro příslušnou prioritu požadavku, od vydání aktualizace výrobcem (např. zveřejnění na portálu výrobce, informační email výrobce, apod.). Požadavek může rovněž založit Objednatel, pokud tuto skutečnost zjistí dříve, kdy následně Helpdesk Objednatele informuje o této skutečnosti domluveným kanálem (email, telefon, Service Desk Zhotovitele) technickou podporu Zhotovitele.</p> <p>Do doby pro Obnovení služby dané prioritou požadavku počítané od okamžiku zveřejnění informace výrobcem musí Zhotovitel poskytnout stanovisko pro vhodnost nasazení v prostředí Objednatele s identifikací možných dopadů, definovat způsob nasazení a provést aplikaci aktualizace či záplaty.</p>
Měřicí bod	Service Desk Objednatele, informační kanál výrobce (portál, informační email, apod.)
Způsob dokladování	Měsíční report o plnění KPI.

Sleva z ceny	700 Kč za každou započatou hodinu nad dobu pro Obnovení Služby stanovenou prioritou požadavku.
Doplňující informace	
Poznámka	-
Platební podmínky	Paušální měsíční cena podle Smlouvy.



5.3. IDM04 Reparametrizace a optimalizace

Katalogové Služby	
Identifikace (ID)	IDM04
Název Služby	Reparametrizace, optimalizace a adaptace Systému pro jeho efektivnější využívání
Popis Služby	On-site asistence, optimalizace a provádění úprav Systému za účelem jeho efektivnějšího, bezpečnějšího a komplexnějšího využívání. Službou je zabezpečeno řešení požadavků na Systém, jejichž příčinou není incident (nefunkčnost).
Parametry	
Název	KPI04 Reparametrizace
Definice	V rámci této Služby jsou vykonávány zejména, nikoliv však výhradně, následující činnosti: <ul style="list-style-type: none"> • realizace rekonfigurací a drobných úprav vedoucích k efektivnějšímu, bezpečnějšímu a komplexnějšímu využívání Systému; • řádné zadokumentování provedených změn <p>Služba bude poskytována podle požadavků Objednatele.</p>
Parametry KPI	
Kalendář Služby	8x5
Definice parametrů	Odmítnutí nebo přijetí požadavku s definováním termínu jeho zpracování do 3 Pracovních dní. Dodržení stanoveného termínu ukončení realizace požadavku. Dodání měsíčního záznamu o poskytnutí Služby (viz níže v tomto KL).
Měřicí bod	Service Desk MZe.
Způsob dokladování	Měsíční záznam o poskytnutí Služby s identifikací poskytnutých činností a služeb, rozpadu pracovní, včetně elektronické verze záznamu ve standardním čitelném formátu. Minimální jednotkou pro dokladování pracovní je hodina na jednoho člověka.
Sleva z ceny	V případě porušení byť i jednoho parametru KPI04 má Objednatel právo na smluvní pokutu ve výši 5.000,- Kč za každé porušení povinnosti. Za porušení parametru KPI04 Zhotovitelem se považuje: <ol style="list-style-type: none"> 1. nedoručení přijetí nebo odmítnutí požadavku Objednatele do 3 Pracovních dnů; 2. v případě přijetí požadavku Objednatele a termínu jeho zpracování, nedodržení této doby zpracování požadavku včetně řádného zadokumentování provedených změn; 3. nedodání měsíčního záznamu o poskytnutí Služby se všemi požadovanými parametry (viz Způsob dokladování)
Doplnění informací	
Objem poskytované Služby	Objem, který je Objednatel oprávněn čerpat, činí 20 člověkodní za období jednoho roku po dobu trvání Podpory definované Smlouvou. Čerpání bude probíhat podle aktuálních potřeb Objednatele.
Platební podmínky	V rámci tohoto katalogového listu budou hrazeny pouze reálně čerpané člověkodny resp. člověkohodiny podle nabídnuté denní sazby za člověkohodinu, a to do maximálního objemu definovaného tímto katalogovým listem. Úhrada bude provedena na základě odsouhlaseného záznamu a pracovní o poskytnutí Služby. Minimální jednotkou pro dokladování pracovní je hodina na jednoho člověka.

PŘÍLOHA Č. 3

TECHNICKÁ SPECIFIKACE



MINISTERSTVO ZEMĚDĚLSTVÍ

Technická specifikace

Poskytnutí IDM řešení

OBSAH

1	Účel dokumentu	55
2	Přehled základních pojmů	56
3	Aktuální stav	57
3.1	Základní procesy nad uživatelskými účty	58
3.2	Import z HR systému	58
3.3	Popis jednotlivých řízených systémů	58
3.3.1	MS Active Directory	59
3.3.2	MS Exchange	59
3.3.3	LDAP (Oracle Internet Directory – OID)	59
3.3.4	SAP CUA (SAP Central User Administration)	60
4	Požadovaný stav a motivace	61
5	Popis požadovaného řešení	63
5.1	Požadavky k implementaci	63
5.1.1	Import z HR systému	63
5.1.2	Provisioning do řízených systémů	64
5.1.3	Admin rozhraní	64
5.1.4	Integrace se systémem SIEM	64
5.1.5	Notifikace	65
5.2	Požadavky na podporu funkcionality	65
5.2.1	Správa rolí	65
5.2.2	Schvalovací workflow	65
5.2.3	Uživatelské rozhraní	65
5.2.4	Řízení hesel	66
5.2.5	Manuální správa IDM uživatelů	66
5.2.6	Reconsiliace	66
5.2.7	Dávkové operace	66
5.3	Rozsah	67
5.3.1	Počet uživatelů	67
5.3.2	Prostředí	67
5.3.3	Dostupnost	67
5.4	Fáze realizace dodávky	67
5.4.1	Analýza	68
5.4.2	Instalace	68
5.4.3	Implementace	68
5.4.4	Akceptační testy	69
5.4.5	Dokumentace	69

5.4.6 Školení	70
5.5 Podpora	70
5.6 Platformy.....	70
Příloha A – Současné procesy.....	73
A.1. Založení nového uživatele	73
A.2. Změna atributů uživatele.....	74
A.3. Administrátorské uzamčení/odemčení účtu	75
A.4. Administrátorská aktivace účtu uživatele DPP/DPČ.....	76

Seznam obrázků

Obrázek 1 - Současná funkcionalita IDM	57
Obrázek 2 - Oblasti IDM	62

Seznam tabulek

Tabulka 1 - seznam zkratk a pojmů	56
---	----

1 Účel dokumentu

Dokument obsahuje požadavky na implementaci nového IDM systému, který má nahradit současné již zastaralé a nepodporované IDM řešení provozované v prostředí MZe. Záměrem je nahradit stávající řešení v rozsahu funkcionality, která je momentálně implementována. V další fázi bude řešení rozšířeno o další funkcionality, která musí být implementovaným IDM systémem podporována, nebude však v rámci tohoto zadání požadována k nasazení.

Dokument tvoří přílohu zadávací dokumentace veřejné zakázky "Poskytnutí IDM řešení" a obsahuje představení požadovaného konceptu řešení, základní popis poptávaného řešení a požadavky závazné pro všechny potenciální uchazeče o zajištění realizace zakázky.

2 Přehled základních pojmů

Termín	Význam
AD	Microsoft Active Directory
DB	Databáze
DC	Datové centrum
DN	Distinguished name. Unikátní jméno objektu v adresáři typu LDAP.
EP	End Point – řízený koncový systém (Win, Linux, DB, Router, SAP ...)
DRP	Disaster recovery plan
DPČ	Dohoda o pracovní činnosti
DPP	Dohoda o provedení práce
HA	High Availability – režim vysoké dostupnosti (např. redundance)
HPP	Hlavní pracovní poměr
HW	Hard-Ware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IDM	Identity Management – správa uživatelských účtů
LDAP	Lightweight Directory Access Protocol
Objednatel/Zadavatel/MZe	Česká republika – Ministerstvo zemědělství
OID	Oracle Internet Directory – LDAP systém od Oraclu, který je implementován v prostředí MZe
OS	Operační Systém
OSS	Organizační složka státu
RBAC	Role-based access control model popisující restrikcí systémových oprávnění na základě autorizace uživatelů.
SIEM	Security Information and Event Management - správa bezpečnostních informací a událostí
SNMP	Simple Network Management Protocol
SP	Služební poměr
SSO	Single sign on - systém jednotného přihlášení
SUR	Aplikace pro správu uživatelů a rolí
SW	Software
Zhotovitel, Dodavatel	Subjekt, který je jako Zhotovitel/Dodavatel definován v záhlaví Smlouvy

Tabulka 1 - seznam zkratk a pojmů

3 Aktuální stav

Současná implementace IDM pokrývá jednoduchý provisioning uživatelských účtů do řízených systémů. Řízeny jsou pouze účty zaměstnanců, účty externistů a zaměstnanců podřízených organizací jsou řízeny mimo IDM.

Zdroj:

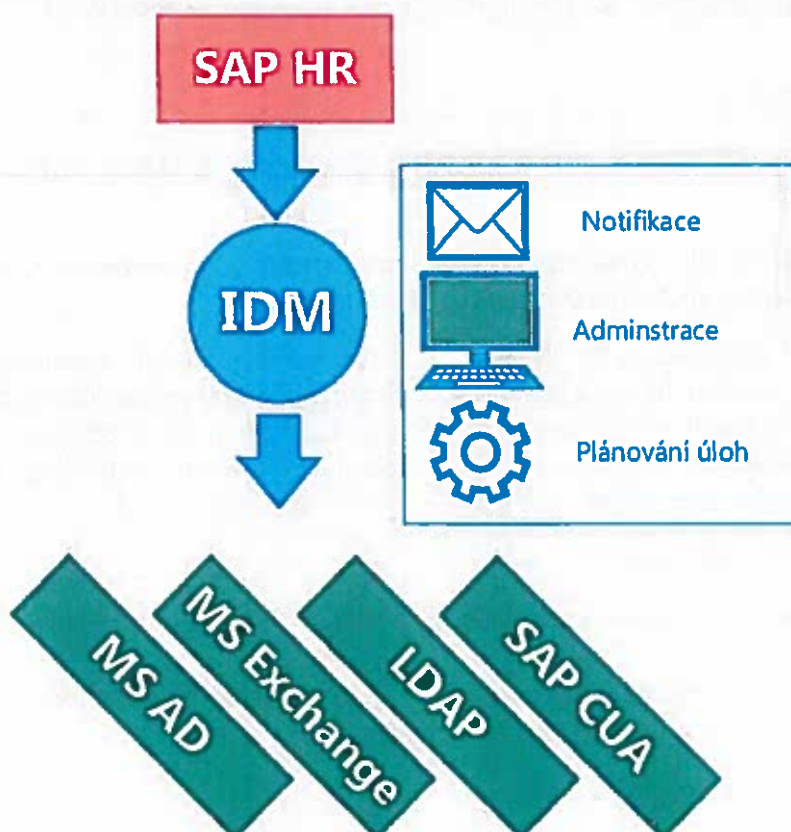
- SAP HR – slouží jako autoritativní zdroj osob/kontraktů

Cíle:

- MS Active Directory – uživatelské účty,
- MS Exchange – emailové schránky pro AD uživatele,
- LDAP (Oracle Internet Directory – OID) – uživatelské účty
- SAP CUA (SAP Central User Administration) – uživatelské účty

Kromě provisioningu výše uvedených systémů z hlavního zdroje, zajišťuje IDM systém následující služby:

- Plánování úloh
- Administrátorské rozhraní umožňující naplánovat, či manuálně spustit úlohu
- Zaslání mailových notifikací na základě konfigurovaných podmínek.



Obrázek 1 - Současná funkcionalita IDM

3.1 Základní procesy nad uživatelskými účty

IDM obsluhuje celkem tři základní IDM procesy:

1. **Založení nového uživatele** – standardní nástup nového zaměstnance.
2. **Změna atributů uživatele** – změna zahrnuje také
 - a. aktivaci/deaktivaci uživatele na základě změny statusu v HR systému,
 - b. změnu emailu při změně jména uživatele.
3. **Administrátorské uzamčení/odemčení uživatele** – používá se buď pro okamžité zablokování aktivního uživatele a všech jeho účtů, nebo pro odblokování jednotlivých účtů neaktivního uživatele na základě speciálního požadavku (např. přístup k mailu bývalého zaměstnance, který přešel do jiné organizace, přesto s MZe spolupracuje na základě jiné dohody).
4. **Administrátorská aktivace účtů uživatele DPP/DPČ** – uživatelé s pracovním poměrem DPP/DPČ jsou zakládány v IDM bez toho, aniž by jim byly vytvářeny uživatelské účty v řízených systémech. Až na základě požadavku provede IDM administrátor aktivaci řízených účtů IDM uživatele, která spustí provisioning účtů do vybraných systémů (prerekvizitou vytvoření všech účtů je existence AD účtu).

Schémata zachycující přibližnou podobu jednotlivých procesů jsou uvedena v kapitole Příloha A (pro přehlednost jsou např. vynechány některé notifikace, které jsou popsány pouze v textu níže).

Jakákoliv změna IDM uživatele je propagována do řízených systémů na příslušné uživatelské účty.

3.2 Import z HR systému

Zdrojovým systémem pro import je SAP HR, který je součástí systému SAP ERP 6.0 EHP6.

Import uživatelů ze SAP HR systému probíhá pomocí vlastního vyvinutého SAP HR konektoru, který volá vlastní vyvinuté BAPI funkce na straně SAPu.

IDM vyčítá informace o jednotlivých uživateliích ze SAP HR systému a porovnává je s vlastními údaji. Jako primární klíč pro identifikaci uživatele a vazbu je použito osobní číslo zaměstnance. Pokud uživatel v IDM není nalezen, je spuštěn proces založení nového uživatele. Pokud je detekován rozdíl mezi informacemi ze SAP HR a IDM, je spuštěn proces změny atributů uživatele v IDM.

Import se spouští ve dvou režimech:

- **Full reconsiliace** – je provedeno porovnání všech zaměstnanců/účtů v SAP HR a IDM
- **Inkrementální reconsiliace** – jsou porovnány pouze uživatelé, na kterých proběhla od posledního importu v SAP HR systému změna.

3.3 Popis jednotlivých řízených systémů

Následuje detailnější popis systémů, které jsou řízeny současným IDM systémem. Jako **uživatelské jméno** je vždy použito osobní číslo zaměstnance, tudíž není nutné generovat unikátní řetězec. Pro žádný z řízených systémů není uživateli nastavováno heslo.

Účty na řízených systémech nejsou nikdy odstraňovány.

3.3.1 MS Active Directory

AD je provozováno na doménových kontrolérech verzi:

- Microsoft Active Directory 2008 R2 SP1,
- Microsoft Active Directory 2012,
- Microsoft Active Directory 2012 R2.

Forest i domény jsou provozovány ve functional level 2003, z důvodu kompatibility se stávajícím IDM systémem. Po migraci na nový IDM systém se předpokládá povýšení functional levelu na verzi 2008 R2.

V AD je IDM systémem řízena jedna doména. Uživatelé jsou automaticky vytvářeni/aktualizováni v jednom kontejneru. Uživatelům je nastavena sada atributů, které přímo vycházejí z hodnot atributů osoby ze SAP HR systému. Uživatelům je také nastaveno členství v základních AD skupinách dle definovaných podmínek (typ zaměstnance, členství v org. jednotce).

V AD je dohledán manažer IDM uživatele dle osobního čísla, které je dostupné ve vlastním atributu. DN manažera je doplněno do atributu AD uživatele. Pokud manažer není dohledán, je vyplněna defaultní hodnota a je odeslána notifikace.

Nové DN AD účtu je vyplněno do atributu IDM uživatele (a je dále použito při provisioningu LDAP účtu, který má v jednom ze svých atributů právě tuto hodnotu kvůli funkčnosti externí autentizace).

AD je instalováno pouze jako **produkční**, momentálně není k dispozici testovací prostředí. Do doby implementace IDM systému bude **testovací prostředí** připraveno.

3.3.2 MS Exchange

Jedná se o

- Microsoft Exchange Server 2013 CU7.

Po úspěšném založení uživatele v doméně je mu vygenerována unikátní mailová adresa a aktivována mailová schránka. Mailová adresa je uložena také do atributu IDM uživatele.

Při změně příjmení uživatele je vygenerována nová unikátní mailová adresa, která je přidána jako nový primární alias (původní alias je zachován).

Stejně jako v případě AD je také MS Exchange pouze jako **produkční**, bez testovacího prostředí. Do doby implementace IDM systému bude **testovací prostředí** připraveno.

3.3.3 LDAP (Oracle Internet Directory – OID)

Jedná se o

- Oracle Internet Directory 11.1.1.5.0.

K LDAPu je přístupováno standardním protokolem LDAPs. Po úspěšném založení uživatele v AD doméně je založen účet stejného jména v OID. Uživatelé nejsou systémem IDM přidělovány žádné skupiny.

LDAP je instalován celkem ve třech prostředích: **produkční, testovací a vývojové**.

3 3 4 SAP CUA (SAP Central User Administration)

Jedná se o

- SAP CUA, který je součástí SAP Solution Manager SM 7.1 SPS12

System SAP CUA je napojen IDM konektorem vyvinutým na míru. Uživateli je v systému SAP CUA založen neaktivní účet bez hesla a oprávnění se základní sadou atributů, která přímo vychází z atributů IDM uživatele. Uživatel je aktivován a dále nastaven manuálně administrátorem na základě notifikace odeslané IDM systémem.

SAP Solution Manager je instalován celkem ve dvou prostředích: **produkční a testovací**.



4 Požadovaný stav a motivace

IT prostředí MZe je tvořeno velkým množstvím informačních systémů, ke kterým mají přístup zaměstnanci, podřízené organizace, externisté, nebo i široká veřejnost (farmáři). Správa těchto přístupů je klíčová pro provoz organizace jak z hlediska dostupnosti, tak z hlediska bezpečnosti. Většina těchto přístupů je zřizována a dále udržována manuálně operátory MZe, případně částečně automaticky stávajícím IDM systémem nebo jinými vlastními nástroji. Kromě vysokého zatížení operátorů MZe je problémem i chybovost současného způsobu správy. Někteří uživatelé mají zřízené přístupy se značnou prodlevou, což jim znemožňuje pracovat (dostupnost), nebo dochází k ponechání přístupu uživatelům, kteří již odešli, nebo změnili pracovní pozici (bezpečnost).

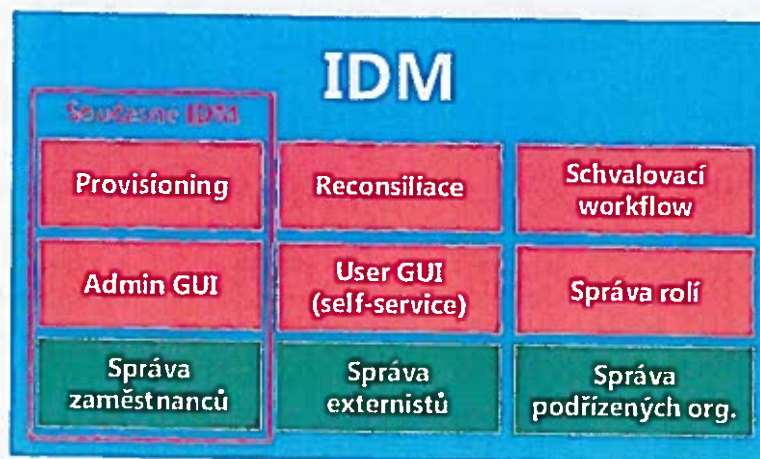
Většina těchto informačních systémů využívá jako zdroj uživatelů Active Directory (AD) nebo LDAP. Tyto zdroje jsou využívány jak k autentizaci uživatelů (přihlašování), tak k autorizaci (přístupy v rámci systémů). Speciální skupinu systémů tvoří systémy SAP. Uživatelé účty v rámci systémů SAP jsou centrálně spravovány komponentou SAP CUA.

Současně provozovaný IDM systém zajišťuje vytváření, aktualizaci a blokaci uživatelských účtů v AD, LDAP a SAP CUA pro zaměstnance MZe (více v kapitole 3). Tento IDM systém již není výrobcem podporován a jeho údržba je pracná a nákladná, navíc trpí velkou chybovostí, která znamená nutnost často manuálně zasahovat do jinak automatických procesů.

Cílem je současný IDM systém co v nejkratší době nahradit novým spolehlivým celistvým IDM systémem, kterým se pokryje funkcionalita současného IDM systému a zároveň bude umožněn další rozvoj, tak aby byla funkcionalita systému rozšířena o správu účtů také pro ostatní skupiny uživatelů, než jsou zaměstnanci, a aby IDM systém také zajišťoval správu oprávnění uživatelů (role).

Předmětem této veřejné soutěže bude pouze fáze nahrazení současného IDM v šířce jeho nasazení. Důvodem je maximální urychlení náhrady nyní provozovaného nepodporovaného řešení, a tím předejití případným organizačním problémům souvisejícím se selháním tohoto systému.

Následující obrázek znázorňuje jednotlivé oblasti, které jsou pokryty současným řešením, a které budou předmětem implementace v rámci této zakázky „Poskytnutí IDM řešení“ a také ostatní oblasti, které musejí být nabízeným řešením podporovány tak, aby bylo možné toto řešení jednoduše rozšířit. Popis konkrétních požadavků je uveden v dalších kapitolách.



Obrázek 2 - Oblasti IDM

5 Popis požadovaného řešení

Objednatel v rámci výběrového řízení požaduje zajištění kompletní dodávky IDM systému, který vyhovuje požadavkům uvedeným v této kapitole.

Splnění požadavků bude podloženo předložením **Návrhu technického řešení (dále jen „NTR“)**, v kterém bude nabízené řešení popsáno. Popis řešení bude obsahovat způsob naplnění všech požadavků uvedených v následujících kapitolách 5.1 a 5.2, a z tohoto popisu bude jednoznačně zřejmé, že návrh řešení všechny tyto požadavky opravdu splňuje. Popis může být rozšířen o odkaz na příslušnou část dokumentace výrobce, který bude mít pouze účel upřesnění, informace o naplnění požadavku musí být zřejmá již ze samotného popisu.

Požadavky jsou rozděleny do dvou skupin dle toho, zda bude požadováno jejich nasazení v rámci dodávky, nebo bude vyžadována pouze jejich nativní podpora v rámci nabízeného řešení. **Nativní podporou se myslí to, že je funkcionální standardní součástí dodávaného IDM systému a není potřeba dokupování dalších modulů nebo dodatečného vývoje.**

5.1 Požadavky k implementaci

IDM systém bude instalován a konfigurován v prostředí MZe tak, aby obsluhoval současné základní IDM procesy organizace, zmíněné v odstavci 3.1. Tyto procesy budou v rámci analýzy revidovány dodavatelem a jejich finální podobu schválí zadavatel. Účel revize je primárně zjednodušení stávajících procesů, jejichž podoba je částečně ovlivněna možnostmi současného IDM řešení.

Implementaci je možné rozdělit do několika funkčních částí, které jsou dále rozepsány.

5.1.1 Import z HR systému

Import uživatelů bude realizován načítáním CSV souboru, který bude v pravidelném intervalu exportován SAP HR systémem do vybrané sdílené složky.

Importované osoby/kontrakty jsou celkem čtyř typů:

1. HPP - Hlavní Pracovní Poměr
2. SP – Služební poměr
3. DPČ - Dohoda o Pracovní Činnosti
4. DPP - Dohoda o Provedení Práce

IDM systém bude automaticky zakládat účty v řízených systémech pouze pro kontrakty typu SP a HPP. Jedna osoba může mít maximálně jeden SP nebo HPP, může mít však více poměrů DPČ/DPP. Proto nejsou účty na koncových systémech pro kontrakty typu DPČ/DPP zakládány automaticky, ale jsou pouze (před)vytvořeny v IDM systému a až na základě potvrzení administrátorem je pro takového IDM uživatele vytvořen uživatelský účet ve vybraném řízeném systému (administrátor zvolí v jakých řízených systémech bude účet vytvořen).

V rámci importního procesu je implementován ochranný mechanismus, který přeruší import v případě, že je detekován příliš velké množství změn, přičemž tento počet je definován jako konfigurovatelný parametr.

5.1.2 Provisioning do řízených systémů

Uživatelům importovaným do IDM systému jsou provisionovány uživatelské účty do řízených systémů, dle nastavených pravidel, která přímo vycházejí z popsaných procesů.

Provisioning bude implementován tak, aby odpovídal aktuálnímu stavu, popsaném v odstavci 3.3. V rámci dodávky budou tedy napojeny následující 4 systémy:

1. Microsoft Active Directory
2. Microsoft Exchange
3. LDAP (OID)
4. SAP CUA

Před samotným napojením řízených systémů bude provedeno mapování IDM uživatelů na existující uživatelské účty na řízených systémech. Mapování bude probíhat podle jednoznačného uživatelského jména, které je v podobě čísla zaměstnance. Toto mapování bude Objednateli předloženo k revizi a až po jeho schválení bude realizováno v IDM systému.

Integrace na každý z řízených systémů bude podporovat speciální pilotní režim, v rámci kterého nebudou do řízeného systému propagovány žádné změny (budou read-only), budou pouze logovány, tak aby mohla být provedena analýza chování provisioningu a nebyl přítom ohrožen provoz těchto napojených řízených systémů.

5.1.3 Admin rozhraní

Dodaný IDM systém bude disponovat webovým administrátorským rozhraním, prostřednictvím kterého bude administrátorům umožněno provádět následující akce:

- Přehled IDM uživatelů, včetně jejich účtů spravovaných na koncových systémech.
- Okamžitá blokace IDM uživatele, včetně jeho navázaných účtů. Tato blokace nebude ovlivněna HR importem.
- Aktivace IDM uživatele, který byl zablokovan HR importem. Tato aktivace nebude ovlivněna HR importem.
- Aktivace konkrétního účtu na koncovém systému, který je navázán na neaktivního IDM uživatele. Tato aktivace nebude ovlivněna HR importem.

Veškeré tyto administrátorské akce budou řádně auditovány a budou přeposílány spolu s ostatními auditními logy do systému SIEM (viz další odstavec).

Webové admin rozhraní musí být kompatibilní s prohlížečem:

- Internet Explorer ve verzi 10 a vyšší.

5.1.4 Integrace se systémem SIEM

IDM systém loguje jak veškeré aktivity prováděné administrátory, tak i veškeré automatické operace nad uživateli IDM a účty v řízených systémech prováděné IDM systémem. Všechny tyto logované záznamy jsou v reálném čase přenášeny do systému pro bezpečnostní monitoring (SIEM) k jejich vyhodnocení a uložení na centrálním bezpečném místě pro případnou zpětnou analýzu.

Události je možné vyčítat systémem SIEM jednou z následujících metod:

- Syslog
- SNMP TRAP

- Textový soubor
- JDBC
- Microsoft Event Log

5.1.5 Notifikace

Součástí IDM systému je notifikační engine, který umožňuje naplánovat mailové notifikace na základě definovaných událostí. Objednatel má k dispozici rozhraní, pomocí kterého může libovolně měnit obsah notifikačních mailů nebo adresátů. Dále je mu umožněno notifikace deaktivovat nebo znovu aktivovat.

V rámci dodávky budou nastaveny následující notifikace:

1. Notifikace o založení nového uživatele do SAP CUA
2. Notifikace o zamknutí účtu v SAP CUA
3. Notifikace o odemknutí účtu v SAP CUA
4. Notifikace o založení IDM uživatele
5. Notifikace o vytvoření nového emailového účtu
6. Notifikace o vytvoření nového účtu v MS AD
7. Notifikace o novém uživateli bez platného manažera
8. Notifikace o odpojení mailboxu

5.2 Požadavky na podporu funkcionality

Následuje popis požadavků na funkcionalitu, která musí být dodaným IDM systémem nativně podporována, nebude však vyžadována v rámci dodávky k implementaci.

5.2.1 Správa rolí

IDM systém umožňuje definovat role, které se skládají ze sady oprávnění v řízených systémech (např. skupiny v LDAPu), nebo ze skupiny jiných rolí (zanořené role). Přiřazením role IDM uživateli, získá uživatel oprávnění v řízeném systému odpovídající sadě oprávnění takové role, případně sady oprávnění všech zanořených rolí. Pokud IDM uživatel nemá žádnou roli, která by mu přiřazovala oprávnění v konkrétním řízeném systému, nebude takový uživatel disponovat aktivním účtem v tomto systému.

Systém umožňuje definovat pravidla, na základě kterých jsou uživatelé automaticky přiřazováni do rolí (resp. odebráni z rolí).

5.2.2 Schvalovací workflow

Součástí systému je workflow engine, který umožňuje definovat a spouštět schvalovací procesy pro přidělování rolí, případně jiné aktivity. Je možné definovat víceúrovňové schvalování, ve kterém jako schvalovatel figuruje buďto konkrétní uživatel, nebo skupina uživatelů/členové role.

Systém podporuje tzv. automatické schvalování – pokud je žadatel zároveň schvalovatel, není toto schvalování vyžadováno a je automaticky označeno jako schválené.

5.2.3 Uživatelské rozhraní

IDM systém poskytuje kromě administrátorského rozhraní také webové uživatelské rozhraní umožňující všem IDM uživatelům základní self-service zahrnující:

- Kontrola hodnot vlastních atributů, přiřazených rolí a vlastních řízených účtů

- Podání žádosti o přiřazení role (výběr role z katalogu rolí)
- Změna vlastního hesla (včetně hesel účtů v řízených systémech)

Uživatelé, kteří figurují jako schvalovatelé rolí (vlastník role, security manažer, nadřízený, atp.) mohou v tomto rozhraní provádět navíc akce:

- Schválení/zamítnutí žádosti o roli
- Přehled žádostí ke schválení, včetně těch, které byly již odbavené
- Přehled podřízených uživatelů (atributy, role)

Systém umožňuje řídit oprávnění v rámci webového uživatelského rozhraní IDM systému. V systému lze definovat alespoň následující uživatelské role:

- Administrátor – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému
- Operátor – systém má přístupný na čtení a je mu umožněno několik základních operací nad uživateli (reset hesla, blokace, atp.)
- Uživatel – základní funkce self-service

Webové uživatelské rozhraní musí být kompatibilní s prohlížečem:

- Internet Explorer ve verzi 10 a vyšší.

5.2.4 Řízení hesel

IDM systém umožňuje definovat různé politiky hesel, které určují složitost hesla. Tyto politiky hesel lze přiřazovat jednotlivým řízeným systémům nebo samotnému IDM systému, takže jsou při změně hesel z IDM rozhraní aktivně vynucovány.

5.2.5 Manuální správa IDM uživatelů

IDM systém nabízí možnost správy IDM uživatelů, kteří nejsou importováni z HR systému. Jedná se o skupinu uživatelů (např. externisté), kteří jsou do IDM systému zakládáni ručně IDM operátorem. Veškerá obsluha je prováděna z webového uživatelského rozhraní, v kterém je umožněno provádět následující akce:

- Založení IDM uživatele
- Aktualizace IDM uživatele
- Deaktivace/Aktivace IDM uživatele

Tito uživatelé nejsou nijak ovlivněni HR importem.

5.2.6 Reconsiliace

Systém podporuje tzv. reconsiliaci řízených systémů, tedy proces, v rámci kterého jsou porovnány skutečné účty s jejich předpokládaným obrazem vypočteným IDM systémem. Výsledkem je buď automatická akce v podobě opravy, nebo notifikace.

V rámci tohoto procesu jsou také identifikovány účty na řízeném systému, které nemají svůj protějšek v IDM systému.

5.2.7 Dávkové operace

Systém poskytuje rozhraní pro dávkový import/export IDM objektů (uživatel, účet, role, oprávnění, vazby mezi objekty, ...).

5.3 Rozsah

V této sekci je definován rozsah dodávaného řešení.

5.3.1 Počet uživatelů

Počet IDM uživatelů importovaných z HR systému:

- Celkový počet uživatelů: 1200;
- Počet přistupujících IDM administrátorů: 5;

Licence potřebné k pokrytí výše uvedených parametrů budou součástí dodávky.

5.3.2 Prostředí

V rámci dodávky je požadována instalace dvou prostředí IDM systému:

- **Produkční**
- **Testovací** (které zároveň slouží jako vývojové)

Požadavky na produkční prostředí vyplývají z této Technické specifikace.

Vývojové/testovací prostředí bude sloužit k testování patchů a nových verzí systému dodaných výrobcem. Zároveň v něm bude probíhat vývoj a testování funkcionalit v rámci rozšiřování systému (konektory, schvalovací WF, integrace, atp.).

Testovací/vývojové prostředí musí zajistit všechny požadované funkční parametry jako prostředí produkční a musí obsahovat minimálně po jedné z komponent použité v produkčním prostředí, aby tak obě prostředí byla identická z pohledu podporovaných funkcí a komponent, a bylo tak možné v testovacím/vývojovém prostředí řádně otestovat veškeré funkcionality a vlastnosti konfigurovatelné v produkčním prostředí.

Všechny změny v rámci IDM systému, zejména upgrade, bezpečnostní záplaty, nové funkcionality a další nové verze IDM systému nebo jeho částí, musí být řádně otestovány Dodavatelem, ještě před nasazením do produkčního prostředí Objednatele. V rámci Poskytnutí IDM řešení se produkční prostředí považuje za testovací až do fáze akceptačních testů (etapa B6. dle harmonogramu).

5.3.3 Dostupnost

Není vyžadována vysoká dostupnost IDM systému. Je však požadováno zajištění kompletní obnovy systému v případě jeho výpadku. Součástí dodávky bude příprava následujících dokumentů:

- Zálohovací plány a postupy
- Opatření a dokumentace k zajištění kontinuity provozu (vč. plánů obnovy Systému)
- Postupy pro obnovení dat včetně konfigurací do původního provozního stavu

Plán obnovy (DRP) bude navržen tak, aby zajistil kompletní obnovu systému v případě výpadku do 4 hodin.

5.4 Fáze realizace dodávky

Následuje popis jednotlivých fází dodávky IDM systému.

5.4.1 Analýza

Dodavatel v rámci dodávky provede nejprve analýzu nezbytnou pro instalaci a konfiguraci komponent IDM systému, integraci všech řízených systémů (viz. 3.3) a připraví technický popis řešení, instalační postup, detailní časový harmonogram a definuje nároky na součinnost. Na základě požadavků na IDM systém Dodavatel připraví návrh testovacích scénářů, pokrývajících testování všech funkčních rysů implementovaného řešení, včetně testování vybraných výkonových parametrů a výpadků jednotlivých komponent. Dále Dodavatel připraví návrh integrace IDM řešení do provozního a bezpečnostního (SIEM) monitoring systému Objednatele.

Všechny požadované výstupy z etapy Analýza budou Objednateli předloženy k odsouhlasení. Objednatel prostuduje předložené výstupy a bez zbytečného odkladu posoudí, zda navrhované řešení splňuje všechny požadované vlastnosti dané touto Technickou specifikací. Pokud Objednatel shledá nesoulad nebo nejasnosti navrhovaného řešení oproti této Technické specifikaci, požádá Dodavatele o nápravu. Teprve po akceptaci bez výhrad všech požadovaných výstupů Objednatelem je etapa Analýza považována za ukončenou a Dodavatel tak může pokračovat v realizaci dodávky následnou etapou Instalace v souladu s odsouhlasenými výstupy z etapy Analýza. Akceptační řízení bude probíhat dle parametrů uvedených v čl. 4 Smlouvy, nedohodnou-li se smluvní strany jinak.

5.4.2 Instalace

Instalace IDM systému bude provedena do vyhrazené bezpečnostní infrastruktury Objednatele, která je založena na virtuální platformě VMware. V případě nemožnosti instalace do virtuálního prostředí, zajistí Dodavatel fyzické umístění a instalaci všech HW komponent řešení do místa určení v prostředí Objednatele jako součást dodávky IDM systému. SW prostředky dodané v rámci IDM systému budou instalovány v poslední verzi dostupné v době plnění. Dodavatel dále zajistí nasazení a aktivaci všech licencí a licenčních klíčů. Architektura instalovaného IDM systému, včetně identifikace komponent, přehledu instalovaných verzí a použitých licencí a licenčních klíčů bude součástí instalační dokumentace.

5.4.3 Implementace

V rámci fáze implementace bude Dodavatelem zajištěna konfigurace IDM systému tak, aby řešení vyhovovalo požadavkům uvedeným v Technické specifikaci.

Jako součást dodávky bude provedeno:

- Konfigurace komponent IDM systému;
- Integrace na SAP HR systém jako na autoritativní zdroj IDM uživatelů;
- Integrace řízených systémů zmíněných v odstavci 5.1.2 (nejprve na testovací prostředí systémů, poté v pilotním režimu na produkci);
- Příprava a publikace webového admin rozhraní;
- Vytvoření notifikací zmíněných v odstavci 5.1.5;
- Integraci IDM systému do provozního a bezpečnostního monitoringu provede Objednatel za součinnosti Dodavatele;
- Nastavení zálohování konfigurace a dat IDM systému;

5.4.4 Akceptační testy

V rámci analytické fáze budou Dodavatelem navrženy testovací scénáře, které budou pokrývat následující oblasti a parametry řešení:

- Funkční testy

Funkční testy ověří, že implementovaný IDM systém poskytuje bezchybně všechny požadované funkcionality uvedené v Technické specifikaci.

- Zátěžové testy

Jejich úkolem je ověřit, že implementované komponenty jsou schopny fungovat s požadovaným množstvím uživatelů bez výrazného dopadu na kvalitu a odezvu řešení.

Testování bude provedeno Objednatelem za součinnosti Dodavatele. Dodavatel k realizaci testů zajistí:

- Nástroje a komponenty potřebné pro testování;
- Přípravu návrhu testování a hodnotících kritérií;
- Přípravu testovacích scénářů;
- Přípravu prostředí a testovacích dat (v součinnosti s Objednatelem);
- Testovací protokoly s výstupy testů;
- Seznam defektů a způsob a harmonogram jejich odstranění;

Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad. Po odstranění podstatných vad budou akceptační testy celé opakovány a ověří tak kvalitu předávaného IDM systému. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Podstatné vady jsou vady, které způsobují tak závažné problémy, že Objednatel nemůže produkt nebo jeho klíčovou část používat či ovládat.

5.4.5 Dokumentace

Dokumentace dodaná v rámci řešení bude obsahovat jak originální dokumentaci dodávanou výrobcem IDM systému, tak i dokumenty popisující nasazení IDM systému v prostředí Objednatele.

Oficiální dokumentace výrobce IDM systému bude předána v elektronické podobě (formát PDF nebo MS Word) a bude provedena v českém, nebo anglickém jazyce. Dokumentace od výrobce musí pokrývat minimálně následující oblasti:

- popis architektury;
- instalace řešení;
- administrace řešení;
- uživatelská příručka;

Dokumentace popisující nasazení IDM systému v prostředí Objednatele musí být předána v elektronické podobě ve formátu MS Word a bude provedena v českém jazyce. Minimální požadavky na rozsah a obsah dodávané dokumentace je následující:

- Instalační dokumentace
 - Popis architektury;
 - Komunikační matice komponent;
 - Instalované verze;

- Licence;
- Instalační postup;
- Implementační dokumentace
 - Popis nastavení komponent IDM systému;
 - Popis způsobu integrace (jednotlivých typů řízených systémů, HR);
 - Popis konfigurace zálohování IDM systému;
- Administrátorská příručka
 - Popis uživatelského rozhraní IDM systému z pohledu administrátora;
 - Popis základních úkonů nutných pro údržbu IDM systému a standardní profylaktické testy;
- Zajištění kontinuity provozu
 - Popis postupu obnovy ze zálohy;
 - Popis postupu v případě havárie jednotlivých komponent včetně postupu obnovy do provozního stavu;

5.4.6 Školení

Dodavatel zajistí proškolení minimálně 3 osob Objednatele na úrovni administrace řešení v rozsahu umožňujícím provádět:

- Běžný rutinní provoz a údržbu dodávaného IDM systému, včetně provedení příslušných konfiguračních změn;
- Řešení obvyklých problémů;
- Správu IDM uživatelů (blokace, aktivace);
- Monitoring stavu zařízení;
- Zálohování a obnovu konfigurace a dat;

5.5 Podpora

Dodavatel ručí za to, že IDM systém bude funkční a použitelný v prostředí Objednatele a bude odpovídat požadavkům Objednatele uvedených v Technické specifikaci a vlastnostem deklarovaným v dokumentaci dodané Dodavatelem. Služby poskytované Dodavatelem musí vyhovovat technickým specifikacím a požadavkům výrobce.

Podpora bude poskytována dle parametrů definovaných ve Specifikaci katalogových listů viz Příloha č.2 Smlouvy a bude probíhat v českém jazyce, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě jinak.

Odstraňování vad technických prostředků bude Dodavatelem prováděno výměnným způsobem na místě s tím, že náhradní díl nebo zařízení musí být nové a bezvadné a musí být doručeny do místa provádění opravy.

5.6 Platformy

Pokud to bude IDM systémem podporováno, bude instalováno do virtuální VMware infrastruktury Objednatele. Systémy jsou pod správou MZe, dodavatelé budou poskytnuty pro instalaci a provoz IDM systému v počtu a kapacitě odpovídající nárokům dodávaného systému, který je dostatečně optimalizován tak, aby neplýtvал prostředky.

Součástí nabídky tak musí být:

- specifikace počtu požadovaných virtuálních serverů a jejich parametrů s ohledem na dostatečnou výkonnost řešení a současnou adekvátnost parametrů;

- specifikace požadavků na parametry komunikačních tras a síťových přístupů mezi jednotlivými komponentami IDM systému;

Pokud není možné IDM systém či jeho komponentu/komponenty provozovat ve virtuálním prostředí, budou součástí nabídky i HW prostředky, které však musí být vybaveny přípojkami pro minimálně dva nezávislé přívody napájení a předozadní větrání.

Veškeré SW licence potřebné k provozu IDM systému (např. OS, DB) musí být součástí dodávky. Výjimku tvoří licence na operační systémy **MS Windows Server** a **Red Hat linux**, které má Objednatel k dispozici a může je pro účel instalace IDM systému poskytnout. Seznam všech dodaných licencí bude součástí nabídky.

Veškeré dodané komponenty (SW, HW) budou instalovány v konfiguraci podporované výrobcem/výrobci, v konfiguraci zaručující vzájemnou kompatibilitu všech komponent a dostatečně výkonnostně nadimenzované s ohledem na parametry požadované od IDM systému.

Veškerý dodaný software (včetně databázi, OS, apod.) bude plně ve správě dodavatele a je poskytnuta jeho podpora dle parametrů definovaných ve Specifikaci katalogových listů, viz Příloha č.2 Smlouvy. Pokud bude využit operační systém **MS Windows Server**, nebo **Red Hat linux** poskytnutý Objednatelem, zůstane takový systém ve správě Objednatele.

IDM systém musí být v souladu s interní směrnicí Objednatele „Definice závazné architektury a požadavků pro vývoj a zabezpečení provozu registrů a klíčových aplikací MZe“ (interní směrnice není přílohou zadání, bude Dodavateli k dispozici v rámci projektu - výňatek s přehledem preferovaných technologií je uveden níže).

Důvodem tohoto požadavku je zajištění kompatibility se stávající infrastrukturou Zadavatele a zároveň možnost využití stávajících mechanismů (HW/SW nástroje, personál, servisní smlouvy) pro správu a monitoring dodaných komponent řešení a jednotného přístupu, bez potřeby dalších investic na straně Zadavatele.

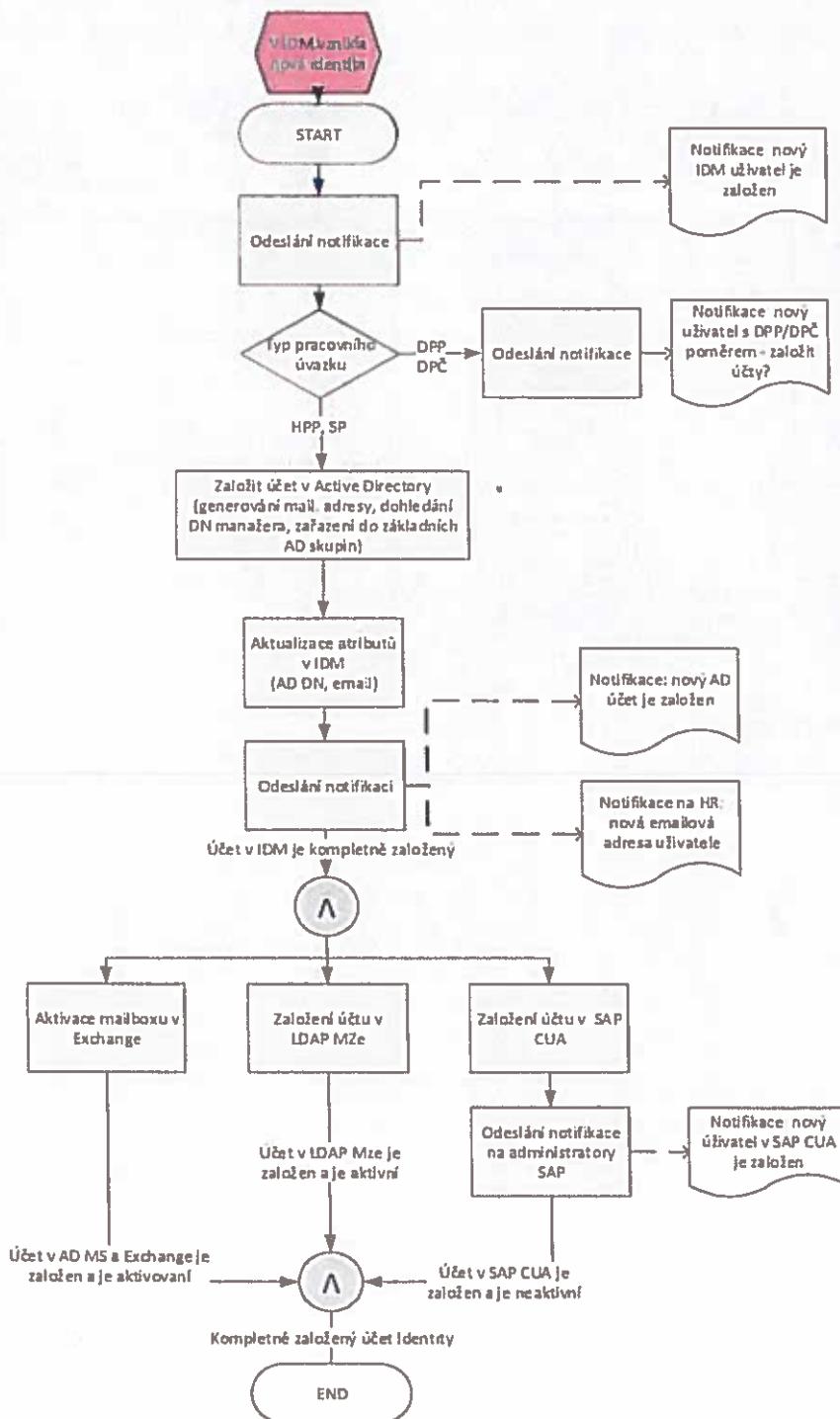
Níže je vykopírován přehled platforem ze zmíněné směrnice:

- Síťové technologie
 - WAN, LAN, HW balancery – technologie Cisco, HP, F5;
 - Firewally, SSL akcelerátory – technologie Cisco, Citrix, HP, F5;
 - SAN prvky – technologie Cisco, HP, Brocade;
- Databázové systémy
 - RedHat Linux Enterprise rel. 6 a vyšší + Oracle 11g rel. 2 a vyšší;
 - Microsoft SQL server verze 2008 a vyšší (pouze pro technologické platformy neumožňující využití Oracle DB);
- Serverové operační systémy
 - Windows server 2012 R2 a vyšší;
 - Red Hat Enterprise Linux AS release 6 a vyšší (64 bit);
- Technologie pro poštovní služby a autentizaci
 - Aplikační autentizace – LDAP Oracle Internet Directory 10g rel. 2 a vyšší;
 - Poštovní služby – MS Exchange 2013 nebo vyšší;
 - Doménová autentizace a autentizace desktopových aplikací Microsoft v prostředí MZe – MS Active Directory;
- Virtualizační technologie
 - VMware ESX 5.0 a vyšší;
- Aplikační servery

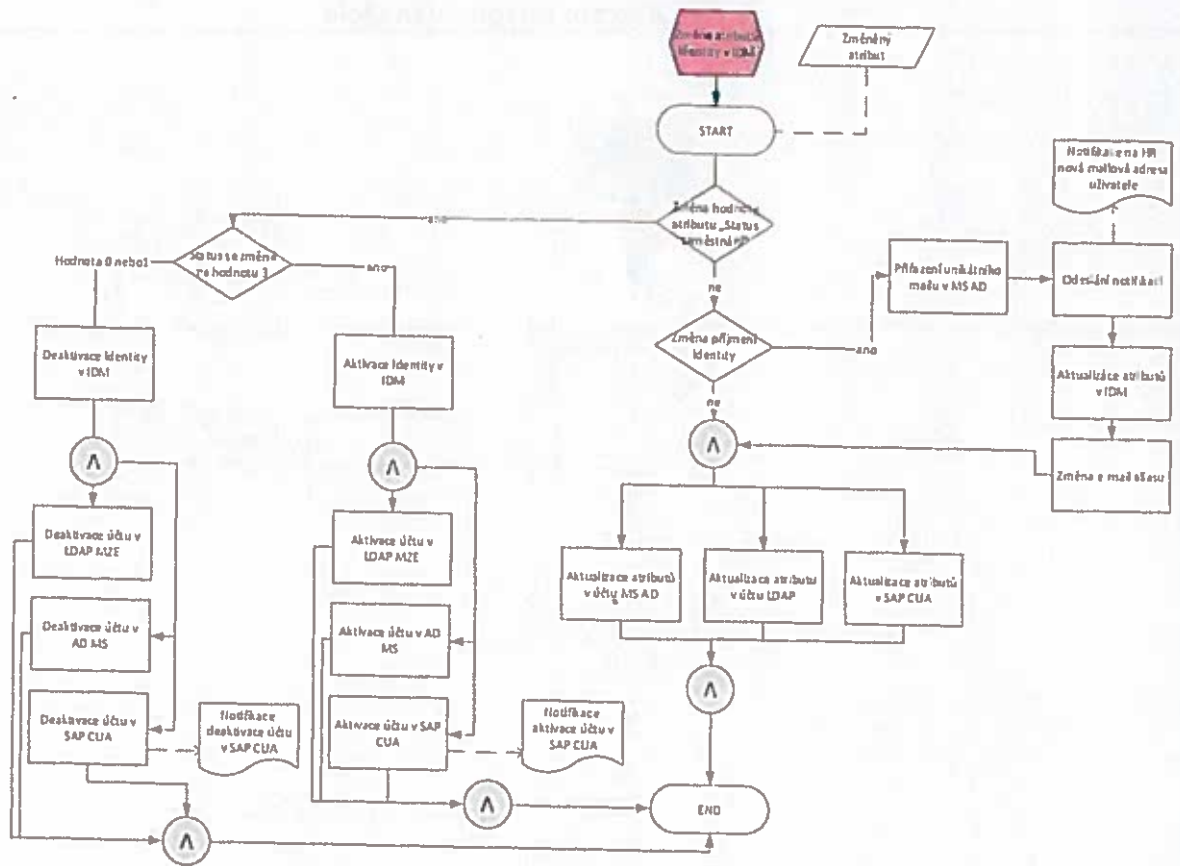
- o Oracle WebLogic Server 11g rel. 1 a vyšší (64 bit) – má vlastní webserver;
- o Microsoft .NET (dot NET) – produkty v rámci MS Internet Information Server 7.0;
- o JBoss – IIS 7.0 a vyšší (win) nebo Apache (linux);
- Prezentační vrstva
 - o Microsoft Internet Explorer verze 10.0 a vyšší.

V případě, že zadávací podmínky této Veřejné zakázky obsahují požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, které platí pro určitou osobu, popřípadě její organizační složku za příznačné, nebo patenty, ochranné známky nebo označení původu, umožňuje Zadavatel výslovně pro plnění Veřejné zakázky použití i jiných, kvalitativně a technicky obdobných řešení, která naplní Zadavatelem požadovanou funkcionalitu (byť jiným způsobem).

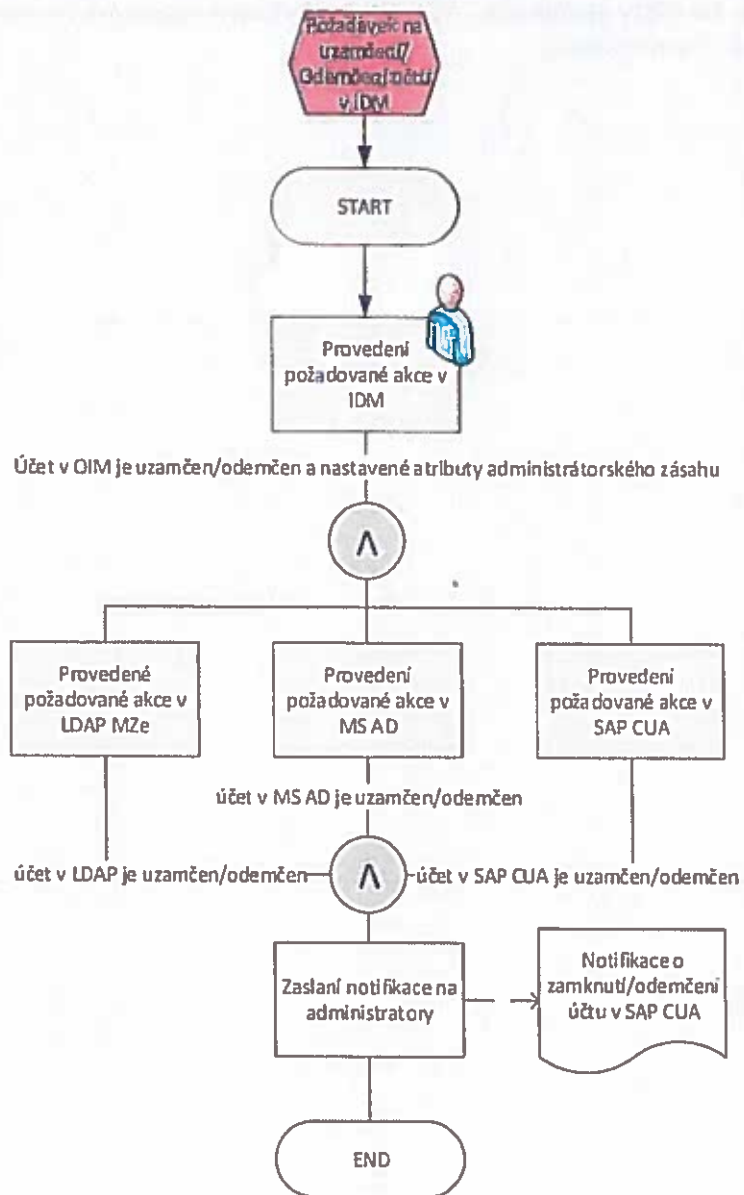
A.1. Založení nového uživatele



A.2. Změna atributů uživatele



A.3. Administrátorské uzamčení/odemčení účtu



A.4. Administrátorská aktivace účtu uživatele DPP/DPČ

Proces odpovídá procesu popsaném v kapitole A.1 Založení nového uživatele pro SP a HPP zaměstnance a pro jednotlivé řízené systémy (prerekvizitou pro vytvoření jakéhokoliv účtu je vždy existence AD účtu). Jediným rozdílem je, že se do cílových systémů nezakládá automaticky.

PŘÍLOHA Č. 4

HARMONOGRAM PLNĚNÍ

Plnění bude realizováno v následujících etapách, které jsou detailněji popsány v Technické Specifikaci:

Etapa	Čas (dny)
B.1. Podpis smlouvy	T
B.2. Analýza	T + 2
B.3. Akceptace Analýzy	T + 3
B.4. Instalace	T + 5
B.5. Implementace	T + 8
B.6. Akceptační testy	T + 9
B.7. Dokumentace	T + 10
B.8. Školení	T + 11
B.9. Akceptace dodávky (platební milník)	T + 12

T = den nabytí účinnosti Smlouvy.

Milník	Termín OD	Termín DO
Maintenance	Ukončení etapy B.4 Instalace	1 rok ode dne „Termín OD“

Milník	Termín OD	Termín DO
Podpora	Akceptace IDM systému	1 rok ode dne „Termín OD“

PŘÍLOHA Č. 5

VZOR PŘEDÁVACÍHO PROTOKOLU

PŘEDÁVACÍ PROTOKOL Č. XXX



P_0127_2015

Projekt

Poskytnutí IDM řešení

Předmět:			
Smlouva č.:	S2015-0055		
Zhotovitel:			
Vypracoval:		Datum:	

Strany předání

Předávající:

Přebírající:

Česká republika – Ministerstvo zemědělství
Těšnov 65/17
110 00 Praha, Česká republika
IČ: 00020478

Předmět předání

Seznam příloh předání

Číslo:	Název přílohy
1	
2	
3	

Schvalovací doložka

Datum převzetí:

Předal:		Převzal:	
Jméno a příjmení		Jméno a příjmení	
Organizace		Organizace	Ministerstvo zemědělství ČR
Podpis		Podpis	



PŘÍLOHA Č. 6

VZOR AKCEPTAČNÍHO PROTOKOLU

AKCEPTAČNÍ PROTOKOL Č. XXX

P_0127_2015



MINISTERSTVO ZEMĚDĚLSTVÍ

Projekt

Poskytnutí IDM řešení

Předmět			
Smlouva č.:	S2015-0055		
Dodavatel:			
Vypracoval:		Datum:	
	Ministerstvo zemědělství		J3AG, s.r.o.
Osoba zodpovědná za akceptaci:			
Předmět akceptace			
Závěry akceptace			
Závěr (akceptováno nebo neakceptováno):			
Způsob akceptace (s výhradami nebo bez výhrad):			
Seznam výhrad akceptace			
Číslo:	Popis výhrady	Termín odstranění	Zodpovědná osoba
1			
Seznam příloh akceptace			
Číslo:	Název přílohy		
1			
2			
3			

Schvalovací doložka			
Jméno a příjmení	Organizace	Podpis	Datum
	Ministerstvo zemědělství		
	J3AG, s.r.o.		



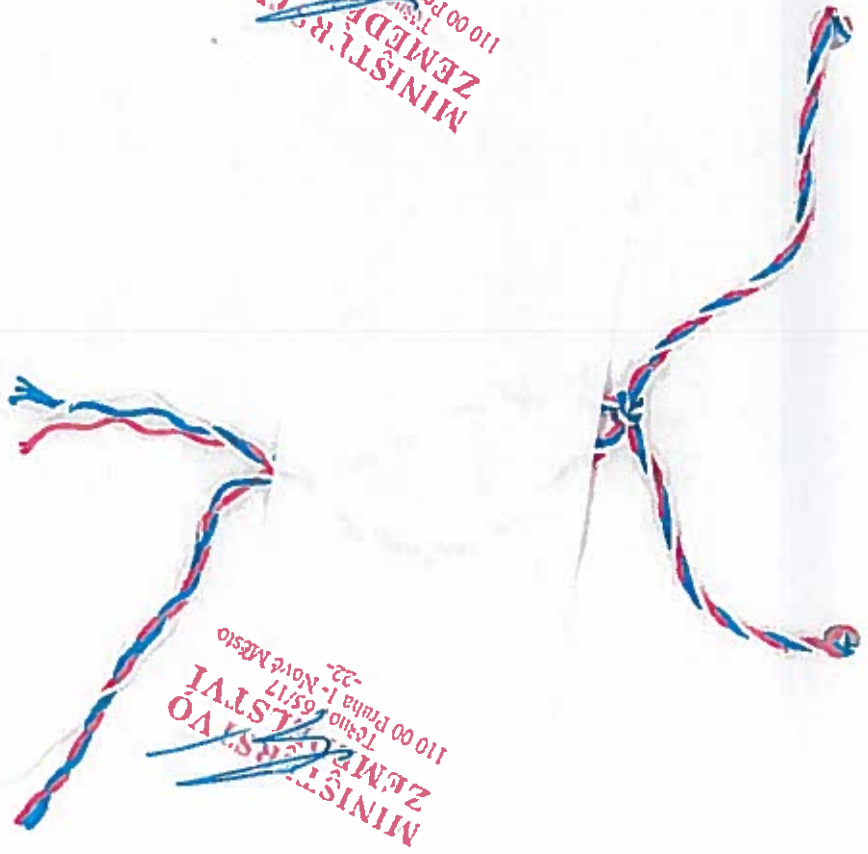
PŘÍLOHA Č. 7

SEZNAM SUBDODAVATELŮ

1/

Název: Orchitech Solutions, s.r.o.
Sídlo: Koněvova 2660/141, 130 00 Praha 3
Právní forma: společnost s ručením omezeným
Identifikační číslo: 28246764
Rozsah plnění Smlouvy: Spolupráce při analýze, instalaci, implementaci, akceptačních testech, dokumentaci, školení a při poskytování následné technické a metodické podpory řešení.

MINISTERSTVO
ZEMĚDĚLSTVÍ
110 00 Praha 1 - Nové Město



MINISTERSTVO
ZEMĚDĚLSTVÍ
110 00 Praha 1 - Nové Město

