**Smlouva na dodání systému Identity managementu**

**NÁRODNÍ ÚSTAV DUŠEVNÍHO ZDRAVÍ**, příspěvková organizace IČO: 00023752

se sídlem Topolová 748, 250 67 Klecany

zastoupena prof. MUDr. Cyrilem Höschlem, DrSc. FRCPsych, ředitelem dále jen **„Objednatel“** na straně jedné

a

### C SYSTEM CZ a.s.

IČO: 27675645

se sídlem Otakara Ševčíka 840/10, 636 00 Brno zastoupen Mgr. Romanem Klimusem, předsedou představenstva

dále jen **„Poskytovatel“** na straně druhé

uzavřeli dnešního tuto smlouvu jako smíšenou smlouvu kupní v souladu s ustanovením §2079 a následujícími, nepojmenovanou v souladu s ustanovením §1746 odst. 2 a smlouvu licenční v souladu s ustanovením §2358 a následujícími zákona č. 89/2012 Sb., občanského zákoníku.

### Preambule

Objednatel provedl v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“) veřejnou zakázku s názvem „Dodávka systému Identity managementu II.“, a to v otevřeném řízení. Zadavatel je příjemcem dotace z fondů Evropské unie prostřednictvím Integrovaného regionálního operačního programu (dále jen

„IROP“), Výzvy č. 23, a to na základě schváleného projektu *„Elektronizace procesů v interních IS NUDZ“*, registrační číslo *CZ.06.3.05/0.0/0.0/16\_028/0006456*. Poskytovatel je osobou v rámci své podnikatelské činnosti oprávněnou a schopnou zajistit dodání systému Identity managementu a poskytnout související služby dle této smlouvy, a to za splnění všech podmínek dle této smlouvy. Tato smlouva je uzavřena na základě výsledků zadávacího řízení a upravuje veškeré smluvní podmínky mezi Objednatelem a Poskytovatelem.

### I.

### Předmět smlouvy

1. Poskytovatel se touto smlouvou zavazuje:
   1. navrhnout, vyvinout a dodat do sídla Objednatele systém Identity managementu a všechny jeho komponenty (dále jen jako „Systém“) a provést jeho implementaci a integraci do stávající architektury Objednatele a do jeho prostředí, včetně zaškolení administrátorů v počtu 3 osob (školení dále jen „Školení administrátorů“);
   2. zajistit pilotní provoz jednotlivých částí Systému prostřednictvím uvedení do zkušebního provozu před jejich předáním Objednateli;
   3. zpracovat veškerou související dokumentaci, která bude nutná pro obsluhu Systému;
   4. importovat iniciální data ze stávajících strukturovaných informačních zdrojů Objednatele;
   5. provést migraci Systému na nový hardware a provést všechny nezbytné úpravy tak, aby byla zajištěna bezproblémová migrace celého Systému do nového prostředí;
   6. poskytnout Objednateli záruku za jakost ve smyslu čl. IV. odst. 3 smlouvy na Systém a s ním spojené plnění, a to v délce pěti (5) let ode dne předání Systému Objednateli;
   7. zajišťovat služby maintenance a supportu Systému v rozsahu dle čl. III. odst. 6 této smlouvy, a to do okamžiku uplynutí pěti (5) let ode dne předání Systému Objednateli ve smyslu čl. III odst. 4 písm. a) smlouvy;
   8. zajistit provedení veškerých analýz, které budou nezbytné pro úspěšnou realizaci projektu, a to mimo jiné analýzu stávajícího workflow a jeho změny po implementaci systému;
   9. poskytnout Objednateli na základě jeho písemné objednávky možnost využití až 400 člověkohodin za účelem konzultačních a programátorských služeb týkajících se provedení individuálních úprav a vylepšení funkcionalit Systému nad rámec požadavků stanovených touto smlouvou, a to po celou dobu účinnosti této Smlouvy, a to dle požadavků Objednatele v souladu s čl. III odst. 7 této smlouvy (dále jen

„Služby rozvoje Systému“);

* 1. poskytnout Objednateli licence specifikované v čl. IX. této smlouvy;
  2. poskytovat Objednateli další služby uvedené v této smlouvě, včetně jejích příloh.

Přesný popis požadavků na dodávku Systému a na provedení dalších souvisejících služeb je specifikován dále v této smlouvě a zejména ve specifikaci obsažené v příloze č. 1 této smlouvy, která je nedílnou součástí této smlouvy (to vše dále jen jako „Předmět plnění“).

Detailní popis a charakteristika systémů využívajících služeb systému je uveden v Příloze č. 2 této smlouvy.

Smluvní strany dále konstatují, že Předmět plnění bude proveden rovněž v souladu s návrhem Poskytovatele, který Poskytovatel zpracoval v rámci podání nabídky v zadávacím řízení a který představuje přílohu č. 4 této smlouvy (dále jen „Návrh Poskytovatele“).

1. Objednatel se touto smlouvou zavazuje Předmět plnění převzít a zaplatit Poskytovateli níže v čl. II. odst. 1. a odst. 2 této smlouvy ujednanou cenu.
2. Poskytovatel se touto smlouvou zavazuje dodat Předmět plnění tak, aby netrpěl faktickými či právními vadami a splnit veškeré povinnosti z této smlouvy včas a řádně. Poskytovatel je povinen zajistit, aby Systém byl schopný rutinního provozu v běžné provozní činnosti s daty Objednatele a aby veškeré výstupy nebo podklady pro výstupy ze Systému byly v souladu s platnou a účinnou legislativou.
3. Poskytovatel prohlašuje, že:
4. dodáním Předmětu plnění neporušuje žádná práva třetích osob, má právo bez omezení s ním nakládat, a tedy i platně převést vlastnické právo k němu touto smlouvou na Objednatele, popř. poskytnout Objednateli licence specifikované v této smlouvě,
5. Předmět plnění bude mít veškeré touto smlouvou ujednané vlastnosti, jakož i vlastnosti obvyklé.
6. Objednatel se touto smlouvou zavazuje poskytnout Poskytovateli ke splnění jeho povinností potřebnou součinnost, tj. zejména převzít Předmět plnění od Poskytovatele v místě plnění, a to pokud bude o takovou součinnost v dostatečném předstihu písemně Poskytovatelem požádán a bude-li Předmět plnění splňovat všechny náležitosti stanovené touto smlouvou.
7. Poskytovatel prohlašuje, že se v potřebném rozsahu seznámil s rozsahem a povahou plnění dle této smlouvy, že jsou mu známy veškeré technické, kvalitativní a další podmínky nezbytné k jeho řádnému poskytování a dodávání a že v tomto směru disponuje nezbytně nutnými kapacitami a odbornými znalostmi. Poskytovatel se zavazuje plnit Předmět plnění dle této smlouvy řádně a včas, a to s odbornou péčí ve smyslu § 5 OZ.

### II.

### Cena a platební podmínky

1. Smluvní strany se dohodly na celkové ceně za Předmět plnění, tj. za plnění dle čl. I. odst. 1 této smlouvy ve výši:

1 120 000 Kč bez DPH,

235 200 Kč odpovídající DPH v zákonné výši, 1 355 200 Kč včetně DPH.

1. Cena dle čl. II. odst. 1 této smlouvy v sobě zahrnuje veškeré náklady, které jsou spojeny se splněním povinností Poskytovatele dle této smlouvy a náklady spojené s plněním

povinností Poskytovatele z vadného plnění (náklady na materiál, ztracený čas servisních techniků, jízdné apod.).

Cena dle čl. II. odst. 1 této smlouvy nezahrnuje cenu za služby maintenance a supportu Systému dle čl. I odst. 1 písm. g) této smlouvy, kdy cena za uvedené služby činí:

200 400 Kč bez DPH za 1 kalendářní rok poskytování služeb maintenance a supportu, 42 084 Kč odpovídající DPH v zákonné výši,

242 484 Kč včetně DPH za 1 kalendářní rok poskytování služeb maintenance a supportu.

Cena dle čl. II. odst. 1 této smlouvy dále nezahrnuje cenu provedení konzultačních a programátorských služeb týkajících se Systému dle čl. I odst. 1 písm. i) této smlouvy, kdy cena za uvedené činí:

1 000 Kč bez DPH za 1 hodinu provedení konzultačních a programátorských služeb dle čl. I odst. 1 písm. i) této smlouvy,

210 Kč odpovídající DPH v zákonné výši,

1 210 Kč včetně DPH za 1 hodinu provedení konzultačních a programátorských služeb dle čl. I odst. 1 písm. i) této smlouvy.

1. Cena dle čl. II. odst. 1 i odst. 2 tohoto článku je ujednána jako nejvýše přípustná, stanovena i s přihlédnutím k vývoji cen v daném oboru včetně vývoje kurzu české měny k zahraničním měnám, a nemůže být ze strany Poskytovatele jednostranně navýšena ani při změnách vnějších podmínek, které nastaly po uzavření této smlouvy. Cena může být překročena pouze v případě změny sazby DPH, a to pouze v rozsahu této změně odpovídajícímu.

Smluvní strany sjednávají, že bližší rozpis Ceny dle odst. 1 a odst. 2 tohoto článku je uveden v rozpočtu, který představuje přílohu č. 3 této smlouvy.

Cena dle čl. II. odst. 1. bude uhrazena na základě a v souladu s podmínkami daňového dokladu – faktury se splatností 30 (slovy: třicet) dnů ode dne jejího doručení Objednateli. Poskytovatel je oprávněn fakturu na částku odpovídající ceně dle čl. I. odst. 1 tohoto článku vystavit až po řádném splnění jeho povinnosti dodat Předmět plnění ve smyslu čl. III odst. 4 písm. a). Nezbytnou přílohou daňového dokladu bude Zápis v souladu s čl. III. odst. 4 písm. a) této smlouvy.

Cena za služby maintenance a supportu Systému dle čl. II. odst. 2 tohoto článku bude uhrazena na základě a v souladu s podmínkami daňového dokladu – faktury se splatností 30 (slovy: třicet) dnů ode dne jejího doručení Objednateli. Poskytovatel je oprávněn fakturu za poskytování služby maintenance a supportu Systému vystavit vždy čtvrtletně, a to až po řádném splnění jeho povinnosti poskytnout služby maintenance a supportu Systému v rozsahu ustanovení čl. I. odst. 1 písm. g) za příslušné kalendářní čtvrtletí. Nezbytnou přílohou daňového dokladu bude Zápis v souladu s čl. III. odst. 4 písm. c) této Smlouvy.

Cena za konzultační a programátorské služby dle odst. 2 tohoto článku bude uhrazena na základě a v souladu s podmínkami daňového dokladu – faktury se splatností 30 (slovy: třicet) dnů ode dne jejího doručení Objednateli. Poskytovatel je oprávněn fakturu za

poskytování konzultační a programátorské služby vystavit vždy čtvrtletně, a to až po řádném splnění jeho povinnosti poskytnout konzultační a programátorské služby v rozsahu ustanovení čl. I. odst. 1 písm. i) za příslušné kalendářní čtvrtletí. Nezbytnou přílohou daňového dokladu bude Zápis v souladu s čl. III. odst. 4 písm. b) této Smlouvy.

1. Daňový doklad – faktura musí obsahovat zejména:
   1. obchodní firmu/název a sídlo Objednatele,
   2. daňové identifikační číslo Objednatele,
   3. obchodní firmu/název a sídlo Poskytovatele,
   4. daňové identifikační číslo Poskytovatele,
   5. evidenční číslo daňového dokladu,
   6. rozsah a předmět plnění,
   7. datum vystavení daňového dokladu,
   8. datum uskutečnění plnění nebo datum přijetí úplaty, a to ten den, který nastane dříve, pokud se liší od data vystavení daňového dokladu,
   9. cenu plnění,
   10. v případě faktury na cenu dle čl. II. odst. 1 a čl. II. odst. 2 v rozsahu fakturace konzultačních a programátorských služeb dle čl. I odst. 1 písm. j) této smlouvy také prohlášení, že účtované plnění je poskytováno pro účely projektu „*Elektronizace procesů v interních IS NUDZ“*, registrační číslo *CZ.06.3.05/0.0/0.0/16\_028/0006456*, a to v rámci Integrovaného regionálního operačního programu (dále jen „IROP“),

a dále veškeré další náležitosti stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

V případě, že daňový doklad tyto náležitosti neobsahuje, popř. že obsahuje chybné údaje, nebo pokud neobsahuje dle povahy fakturovaného plnění Zápis dle čl. III. odst. 4 písm. a)

– c) této Smlouvy, má Objednatel právo Poskytovatele na takový nedostatek upozornit a vyzvat jej k zaslání opraveného daňového dokladu. Po dobu, než bude Poskytovatelem doručen opravený daňový doklad, není Objednatel v prodlení se zaplacením ceny. Zasláním opraveného daňového dokladu běží nová lhůta splatnosti v délce třicet (30) dnů ode dne jeho řádného doručení Objednateli.

4. V případě, že Objednatel přistoupí k reklamaci plnění poskytnutých Poskytovatelem, prodlužuje se splatnost faktury za reklamované plnění o dobu řešení reklamace ze strany Poskytovatele. Dále se splatnost dané faktury prodlužuje v případě, že Poskytovatel nebude akceptovat výsledek reklamačního řízení, a to až do akceptace takového rozhodnutí Poskytovatelem, nebo do případného pravomocného rozhodnutí učiněného soudem.

### III.

### Místo, čas a způsob dodání předmětu plnění

1. Místem plnění je objekt Národního ústavu duševního zdraví, Topolová 748, 250 67 Klecany.
2. Smluvní strany se dohodly, že Poskytovatel je povinen předat Předmět plnění v následujících termínech, kdy jednotlivé úkony uvedené u příslušných termínů jsou blíže specifikovány v Příloze č. 1 této smlouvy:
   1. nejpozději do konce jednoho měsíce ode dne účinnosti této smlouvy je Poskytovatel povinen provést vstupní analýzu používaných systémů;
   2. nejpozději do *121 dnů od nabytí účinnosti této smlouvy* je Poskytovatel povinen zahájit pilotní provoz Systému dle čl. I. odst. I písm. b);
   3. předat do šesti měsíců od nabytí účinnosti Smlouvy Objednateli plně funkční Systém ve smyslu čl. III odst. 4 písm. a) této smlouvy, a to včetně splnění veškerých dalších povinností dle této smlouvy, vyjma těch, které mají být dle své povahy plněny až po předání Systému.
3. Poskytovatel se zavazuje průběžně kontrolovat vydávání nových verzí systému, hotfixů či meziverzí ve smyslu poskytování služby maintenance a supportu dle čl. I odst. 1 písm. g), případně je sám vydávat. V případě že se nová verze systému, hotfix nebo meziverze stane dostupnou, zavazuje se o možnosti její implementace do Systému informovat Objednatele. Poté kdy Objednatel s provedením implementace vysloví souhlas, zavazuje se Poskytovatel zajistit tuto implementaci do Systému. Tato povinnost trvá po celou dobu poskytování služeb maintenance a supportu dle čl. I. odst. 1 písm. g) této smlouvy.
4. Smluvní strany sjednávají, že následující skutečnosti budou vždy potvrzeny písemným Zápisem podepsaným oběma smluvními stranami (dále jen „Zápis“):
   1. Předání Systému pro účely této smlouvy, kde Oboustranně podepsaný písemný Zápis potvrzuje, že došlo k odevzdání Systému Objednateli ve smyslu občanského zákoníku; Objednatel je oprávněn odmítnout převzetí Systému a podpis na Zápisu v případě, že kterákoliv část Systému vykazuje vady, nebo nebyla ve vztahu k tomuto dílčímu plnění splněna kterákoli povinnost uvedená v čl. I. odst. 1 písm. a) - f), h) a j) - k) této smlouvy. V případě že se Objednatel rozhodne převzít Systém s vadami, bude Zápis obsahovat výčet těchto vad, a to včetně přiměřených lhůt pro jejich odstranění.
   2. Řádné splnění povinností Poskytovatele ve smyslu čl. I. odst. 1 písm. i) této smlouvy, kde oboustranně podepsaný písemný Zápis potvrzuje, že došlo k poskytnutí příslušných konzultačních a programátorských služeb za uplynulé kalendářní čtvrtletí. Objednatel je oprávněn odmítnout převzetí konzultačních a programátorských služeb a podpis na Zápisu v případě, že kterákoliv část konzultačních a programátorských služeb vykazuje vady.
   3. Řádné splnění povinností Poskytovatele ve smyslu čl. I. odst. 1 písm. g) této smlouvy, kde oboustranně podepsaný písemný Zápis potvrzuje, že došlo k poskytnutí služeb maintenance a supportu Systému dle čl. I. odst. 1 písm. g) za příslušné kalendářní čtvrtletí. Objednatel je oprávněn odmítnout převzetí uvedených služeb a podpis na Zápisu v případě, že kterákoliv část provedených služeb vykazuje vady.
5. Poskytovatel je při plnění této smlouvy povinen postupovat s odbornou péčí v souladu s platnými právními předpisy, chránit práva a oprávněné zájmy Objednatele. K plnění dle

této smlouvy je Poskytovatel povinen důsledně využívat všechny zákonné prostředky a uplatňovat vše, co podle svého odborného přesvědčení a pokynů Objednatele pokládá za prospěšné. Je přitom vázán pouze zákony a dalšími obecně závaznými právními předpisy České republiky a v jejich mezích také pokyny Objednatele.

1. Poskytovatel se touto smlouvou zavazuje zajišťovat služby maintenance a supportu, a to od okamžiku podpisu Zápisu dle čl. III odst. 4 písm. a) této smlouvy a v případně, že v tomto Zápisu dle čl. III odst. 4 písm. a) této smlouvy budou uvedeny jakékoliv vady nebo nedodělky, pak teprve od okamžiku odstranění všech těchto vad a nedodělků v tomto Zápisu dle čl. III odst. 4 písm. a) této smlouvy uvedených, a to do okamžiku uplynutí pěti

(5) let ode dne podpisu Zápisu dle čl. III odst. 4 písm. a) této smlouvy. Služby maintenance a supportu zahrnují povinnost zajistit činnosti specifikované v Příloze č. 1 této smlouvy a dále zahrnuje provoz informační linky na telefonním čísle, +420731532976 a dále na e- mailové adrese [helpdeskzis@csystem.cz,](mailto:helpdeskzis@csystem.cz) kde budou každý pracovní den v čase od 8:00 do 18:00 s maximální odezvou 60 minut poskytovány Objednateli dle jeho potřeb jakékoliv informace týkající se fungování Systému, přičemž tato informační povinnost trvá po celou dobu poskytování služeb maintenance a supportu dle čl. I. odst. 1 písm. g) této smlouvy. Detailní specifikace služeb maintenance a supportu prováděných na základě této smlouvy je obsažena v Příloze č. 1 této smlouvy.

1. Poskytovatel se touto smlouvou dále zavazuje poskytnout Objednateli možnost využití až 400 hodin za účelem poskytnutí konzultačních a programátorských služeb dle čl. I odst. 1 písm. i), a to dle požadavků Objednatele po předání Systému Objednateli ve smyslu čl. III. odst. 4 písm. a) této smlouvy. Tato časová dotace je určena výhradně pro ty případy, kdy, ačkoliv bude Systém jinak plně funkční, bude mít Objednatel v úmyslu zajistit lepší fungování Systému s ohledem na potřeby jeho provozu a za tím účelem osloví Poskytovatele s žádostí o provedení implementačních, integračních a rozvojových požadavků. Časová dotace ve výši 400 hodin se vztahuje na dobu po předání Systému Objednateli ve smyslu čl. III. odst. 4 písm. a) této smlouvy až doby uplynutí pěti let od předání Systému dle čl. III odst. 4 písm. a) této smlouvy.

### IV.

### Odpovědnost za vady

1. Poskytovatel Objednatele výslovně ujišťuje, že Předmět plnění bude bez vad a bude se hodit k obvyklému účelu. Poskytovatel Objednatele rovněž výslovně ujišťuje, že veškeré práce prováděné v rámci Předmětu plnění budou vykonány s odbornou péčí a budou dosahovat veškerých standardů vyžadovaných právními předpisy.
2. Poskytovatel odpovídá Objednateli za veškeré škody vzniklé porušením povinností vyplývajících z obecně závazných právních předpisů, této smlouvy, technických norem (včetně doporučujících) a z obchodních zvyklostí ze strany Poskytovatele. Za vadné plnění povinností dle této smlouvy a za případnou škodu tímto vadným plněním způsobenou

odpovídá Poskytovatel dle obecně závazných právních předpisů a podmínek stanovených touto smlouvou.

1. Poskytovatel touto smlouvou poskytuje Objednateli smluvní záruku na Předmět plnění v délce trvání 5 (slovy: pět) let. Tato záruka je zahrnuta v ceně, jak je uvedena v čl. II této smlouvy.

Záruční doba počíná běžet dnem podpisu příslušného zápisu dle čl. III. odst. 4 této smlouvy. Poskytovatel tímto Objednateli výslovně zaručuje, že Předmět plnění bude nejméně po dobu odpovídající záruční době způsobilý pro použití v souladu touto smlouvou, s dodanými uživatelskými příručkami a že si zachová vlastnosti vyžadované touto smlouvou, jakož i vlastnosti pro Předmět plnění obvyklé.

1. V případě, že se po dobu trvání této smlouvy vyskytne na jakékoli části Předmětu plnění vada, vyrozumí o tom Objednatel Poskytovatele na e-mailovou adresu uvedenou v čl. VII. odst. 4 této smlouvy, popř. jej o ní uvědomí prostřednictvím webového portálu Poskytovatele. Smluvní strany pro úplnost sjednávají, že Objednavatel je oprávněn vytknout také zjevné vady nacházející se na Předmětu plnění již v době jeho předání, a to kdykoliv po tomto předání, a to aniž by mohl Poskytovatel namítnout, a to i před soudem, že nebyly uplatněny včas.

Postup a lhůty pro odstranění vady jsou stanoveny v čl. 4.6. přílohy č. 1 této smlouvy Strany sjednávají, že odstraněním vady se rozumí též překlenutí vady vytvořením funkčního alternativního řešení, které Objednatel písemně akceptuje, tzv. „workaround“.

V případě výskytu neodstranitelné vady se vždy jedná o podstatné porušení smlouvy a Objednatel má v takovém případě dle své volby nárok na slevu z ceny nebo nárok od smlouvy odstoupit. Vada se ve smyslu této smlouvy považuje za neodstranitelnou, pokud k odstranění vady nedošlo ve lhůtách odpovídajících dvojnásobnému počtu dní, než jak

jsou stanoveny pro jednotlivé typy vad (critical; major; minor; info) v tomto odstavci, resp. příloze č. 1 této smlouvy.

Smluvní strany pro vyjasnění všech pochybností deklarují, že postup dle tohoto odstavce se využije jak pro vady kryté zárukou, tak vady nekryté zárukou, které mají být odstraněny v rámci poskytování služeb supportu a maintenance dle této smlouvy.

1. Záruční doba neběží po dobu, po kterou Objednatel nemůže, z důvodu vady kterékoliv části Předmětu plnění, užívat Předmět plnění v plném rozsahu.
2. Poskytovatel se tímto zavazuje provést Předmět plnění a poskytovat služby dle této smlouvy včetně všech servisních služeb v takové kvalitě, aby byl Systém po jeho předání plně funkční, tj. aby:
   1. netrpěl ani jednou z vad dle odst. 4 tohoto článku, resp. vad dle čl. 4.6. přílohy č. 1 této smlouvy označených jako critical nebo major, a to po 99,9 % času jejího provozu v pracovních dnech v době od 8:00 do 18:00.
   2. netrpěl ani jednou z vad dle odst. 4 tohoto článku, resp. vad dle čl. 4.6. přílohy č. 1 této smlouvy označených jako critical nebo major, a to po 99 % veškerého času, bez ohledu na to, zda jde o pracovní dny v době od 8:00 do 18:00 nebo jakýkoliv jiný den a hodinu.
3. Nároky z vad Předmětu plnění se nedotýkají nároku na náhradu škody nebo nároku na smluvní pokutu.

### V.

### Sankce

1. Smluvní strany nesou odpovědnost za způsobenou škodu v rámci platných právních předpisů a této smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci rozsahu škod již vzniklých.
2. V případě prodlení Poskytovatele se splněním povinnosti poskytovat Předmět plnění v jakémkoliv termínu dle čl. III. odst. 2 této smlouvy se Poskytovatel zavazuje uhradit Objednateli smluvní pokutu ve výši 3.000,- Kč (slovy: tři tisíce korun českých) za každý započatý kalendářní den prodlení s každým termínem.

V případě prodlení Poskytovatele s termínem odstranění Objednatelem uplatněných vad v termínech dle čl. IV. odst. 4, resp. dle čl. 4.6. přílohy č. 1 této smlouvy je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 2.000,- Kč (slovy: dva tisíce korun českých) za každý započatý kalendářní den prodlení s odstraněním každé jednotlivé vady.

V případě prodlení Poskytovatele s poskytováním servisních služeb, tj. v situaci, kdy Poskytovatel nebude řádně plnit veškeré služby maintenance a supportu dle přílohy č. 1 této smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 2.000,- Kč (slovy: dva tisíce korun českých) za každý započatý kalendářní den prodlení s řádným poskytováním služeb maintenance a supportu, a to za každé jednotlivé porušení této povinnosti.

V případě že Poskytovatel poruší povinnost stanovenou v čl. IV. odst. 6. a) této smlouvy takovým způsobem, že Systém po jeho předání nebude v každém kalendářním čtvrtletí plně funkční, tj. že v příslušném kalendářním čtvrtletí bude trpět kteroukoliv z vad dle odst. 4 článku IV, resp. vad dle čl. 4.6. přílohy č. 1 této smlouvy této smlouvy označených jako critical nebo major, a to po více než 0,1 % času jeho provozu v pracovních dnech v době od 8:00 do 18:00, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 2 000

,- Kč (slovy: dva tisíce korun českých) za každé 0,1 % času provozu Systému v příslušném kalendářním čtvrtletí nad limit 0,1 %, po který bude Systém trpět kteroukoliv z vad dle odst. 4 článku IV, resp. vad dle čl. 4.6. přílohy č. 1 této smlouvy označených jako critical nebo major. Smluvní pokuta dle tohoto odstavce může být uplatňována zcela nezávisle a vedle smluvní pokuty dle následujícího odstavce.

V případě že Poskytovatel poruší povinnost stanovenou v čl. IV. odst. 6. b) této smlouvy takovým způsobem, že Systém po jeho předání nebude v každém kalendářním čtvrtletí plně funkční, tj. že v příslušném kalendářním čtvrtletí bude trpět kteroukoliv z vad dle odst. 4 článku IV, resp. vad dle čl. 4.6. přílohy č. 1 této smlouvy označených jako critical nebo major, a to po více než 1 % času jeho provozu bez ohledu na to zda jde o pracovní dny v době od 8:00 do 18:00 nebo jakýkoliv jiný den a hodinu, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 2 000 ,- Kč (slovy: dva tisíce korun českých) za každé 0,1 % času provozu Systému v příslušném kalendářním čtvrtletí nad limit 1 %, po který bude Systém trpět kteroukoliv z vad dle odst. 4 článku IV, resp. vad dle čl. 4.6. přílohy č. 1 této smlouvy označených jako critical nebo major. Smluvní pokuta dle tohoto odstavce může být uplatňována zcela nezávisle a vedle smluvní pokuty dle předchozího odstavce.

V případě porušení povinnosti mlčenlivosti dle čl. VIII této smlouvy je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 100.000,- Kč (slovy sto tisíc korun českých) za každé jednotlivé porušení této povinnosti.

1. Smluvní pokuty dle této smlouvy jsou splatné ve lhůtě 3 (slovy: tří) dnů ode dne doručení výzvy oprávněné smluvní strany straně povinné k jejímu zaplacení.
2. Smluvní pokutu je Objednatel oprávněn započíst na nárok Poskytovatele na úhradu ceny dle čl. II odst. 1 a odst. 2 této smlouvy.
3. V případě prodlení kterékoliv smluvní strany se zaplacením peněžité částky vzniká oprávněné straně nárok na úrok z prodlení v zákonné výši počítaný z dlužné částky za každý i započatý den prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé škody.
4. Povinnost zaplatit smluvní pokutu se nedotýká povinnosti k náhradě škody, ani povinnosti Poskytovatele splnit závazky vyplývající z této smlouvy.

### VI.

### Odstoupení od smlouvy

1. Odstoupit od této smlouvy lze v případech stanovených touto smlouvou nebo zákonem. Smluvní strany pro účely této smlouvy vylučují použití ustanovení § 2111 a § 2112 občanského zákoníku.
2. Objednatel má právo odstoupit od této smlouvy zejména v případě, že:
   1. se Poskytovatel ocitne v prodlení se splněním povinnosti poskytovat Předmět plnění v jakémkoliv termínu dle čl. III. odst. 2 této smlouvy
   2. jakýkoliv dílčí Předmět plnění nebude vykazovat ujednané nebo obvyklé vlastnosti a půjde o podstatné porušení této smlouvy;
   3. Objednatel zjistí, že Poskytovatel neplní nebo s přihlédnutím ke všem okolnostem nebude objektivně schopen řádně a včas plnit své závazky podle této smlouvy;
   4. bude rozhodnuto o úpadku Poskytovatele;
   5. se Poskytovatel ocitne v prodlení s poskytováním služeb supportu a maintenance, tj. v situaci, kdy Poskytovatel nebude řádně plnit veškeré služby supportu a maintenance dle přílohy č. 1 této smlouvy, a takové prodlení neodstraní ani do sedmi dnů poté, kdy k tomu byl vyzván ze strany Objednatele.
   6. Poskytovatel rovněž bere na vědomí, že Předmět plnění veřejné zakázky bude financován z Integrovaného regionálního operačního programu (dále jen „IROP“) v rámci projektu „Elektronizace procesů v interních IS NUDZ“, registrační číslo CZ.06.3.05/0.0/0.0/16\_028/0006456. Poskytovatel bere v tomto směru na vědomí, že Objednatel je oprávněn od této smlouvy odstoupit v celém rozsahu v případě, že na základě pravomocného rozhodnutí dojde k úplnému odnětí, nebo snížení objemu finančních prostředků poskytnutých mu z IROP za účelem pořízení plnění, které je předmětem této smlouvy. Poskytovatel má v takovém případě nárok na úhradu nezbytných nákladů, které byly z jeho strany do okamžiku účinnosti odstoupení prokazatelně a účelně vynaloženy v souladu s touto smlouvou, a to výlučně pokud jde o plnění, které není možné Poskytovateli vrátit v původním stavu.
3. Poskytovatel má právo odstoupit od této smlouvy v případě, že ze strany Objednatele dojde k podstatnému porušení smluvních podmínek stanovených touto smlouvou, za které se pro účely této smlouvy považuje pouze situace, kdy se Objednatel ocitne v prodlení s úhradou jakékoliv části ceny delším než třicet (30) dnů, přičemž byl na toto prodlení písemně upozorněn alespoň deset (10) dnů předtím, než Poskytovatel odstoupil od smlouvy.
4. Odstoupení od smlouvy musí být učiněno písemně a doručeno druhé smluvní straně, přičemž účinky odstoupení nastávají dnem doručení písemného oznámení. Následky odstoupení od smlouvy se řídí příslušnými ustanoveními občanského zákoníku.

### VII.

### Komunikace mezi stranami

1. Za písemnou formu komunikace se považuje osobní doručení, doručení kurýrem, doporučený dopis, faxová zpráva a zpráva poslaná elektronickou poštou podepsaná zaručeným elektronickým podpisem a zpráva doručená datovou schránkou. Za adresy pro doručování písemností se považují adresy smluvních stran uvedené v záhlaví této smlouvy. Změnu adresy pro doručování písemností je třeba vždy oznámit druhé straně bez zbytečného odkladu, a to písemně.
2. Smluvní strany tímto dále sjednávají, že v případech, kdy bude komunikace mezi nimi probíhat e-mailovou formou, budou jednotlivé e-mailové zprávy zasílány na e-mailové adresy smluvních stran uvedené v čl. VII. odst. 4. této smlouvy.
3. Smluvní strany tímto dále sjednávají, že e-mailová zpráva bude považována za doručenou, pakliže druhá smluvní strana její přijetí potvrdí, popř. na tuto zprávu odpoví stejnou formou do tří (3) dnů po jejím odeslání. V opačném případě bude e-mailová zpráva považována za nedoručenou a odesílající smluvní strana bude povinna bez zbytečného odkladu zaslat druhé smluvní straně na její náklady odpovídající zprávu doporučenou poštou prostřednictvím držitele poštovní licence nebo prostřednictvím datové schránky.
4. Pro účely elektronické komunikace označují strany tyto kontaktní emailové adresy: Objednatel: [VYMAZÁNO](mailto:jan.budar@nudz.cz)

Poskytovatel: [VYMAZÁNO](mailto:jan.budar@nudz.cz)

1. Osobami oprávněnými jednat ve věcech této smlouvy jsou následující:

Za Objednatele: Jan Budař, a to v rozsahu podepisování Zápisů dle čl. III. odst. 4, a v rozsahu technických otázek souvisejících s plněním této smlouvy.

Za Poskytovatele: Ing. Kateřina Prettner, a to v rozsahu podepisování Zápisů dle čl. III. odst. 4, a v rozsahu technických otázek souvisejících s plněním této smlouvy.

### VIII.

### Povinnost mlčenlivosti

1. Smluvní strany se zavazují během plnění této smlouvy, stejně jako po jejím skončení, zachovávat mlčenlivost o všech skutečnostech, které se dozví od druhé smluvní strany v souvislosti s plněním této smlouvy. Tím není dotčena povinnost Objednatele uveřejnit tuto smlouvu v příslušném registru smluv, s čímž obě strany vyslovují svůj souhlas.

Poskytovatel tímto zejména bere na vědomí, že v rámci Systému budou uchovávány osobní údaje zaměstnanců i pacientů Objednatele, přičemž ochrana těchto údajů je pro Objednatele naprosto klíčová.

1. Povinnost zachovávat mlčenlivost dle odst. 1 tohoto článku se nevztahuje:
   1. na skutečnosti a informace, které byly v době, kdy byly smluvní straně poskytnuty, veřejně známé,
   2. na skutečnosti a informace, které se stanou veřejně známými poté, co byly smluvní straně poskytnuty, s výjimkou případů, kdy se tyto skutečnosti a informace stanou veřejně známými v důsledku porušení závazků smluvní strany podle této smlouvy,
   3. na skutečnosti a informace, které byly smluvní straně prokazatelně známé před jejich poskytnutím,
   4. na skutečnosti a informace, které je smluvní strana povinna sdělit oprávněným osobám na základě platných právních předpisů,
   5. případy dle odst. 3 tohoto článku.
2. Účastníci této smlouvy berou na vědomí, že Objednatel je povinen dodržet požadavky na publicitu v rámci IROP, a to ve všech relevantních dokumentech týkajících se této smlouvy a dalších dokumentů vztahujících se k plnění dle této smlouvy.

### IX.

### Licenční ujednání

1. Poskytovatel touto smlouvou poskytuje Objednateli licenci k veškerým softwarovým produktům, které tvoří Předmět plnění, a to jako licenci nevýhradní a teritoriálně neomezenou.
2. Licence k užívání Předmětu plnění se poskytuje na dobu trvání padesát (50) let, přičemž odměna za licenci je zahrnuta v ceně dle čl. II odst. 1 této smlouvy.
3. Licence dle tohoto článku zahrnuje neomezený počet přístupů pro zaměstnance a jiné pracovníky Objednatele dle požadavků uvedených v příloze č. 1 Smlouvy.
4. Objednatel není povinen licenci využít.

### X.

### Další práva a povinnosti smluvních stran

1. Poskytovatel se dále zavazuje:
   1. bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky plnění dle této smlouvy; zejména je povinen neprodleně písemně oznámit Objednateli významné změny svého majetkoprávního postavení, jako je např. přeměna společnosti, snížení základního kapitálu, vstup do likvidace, úpadek či prohlášení konkurzu;
   2. informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách majících vliv na plnění dle smlouvy, byť by za ně Poskytovatel neodpovídal, o vznesených požadavcích orgánů státního dozoru a o uplatněných nárocích třetích osob, které by mohly plnění ovlivnit;
   3. poskytnout Objednateli veškerou nezbytnou součinnost k naplnění účelu smlouvy;
   4. na žádost Objednatele spolupracovat či poskytnout maximální součinnost dalším poskytovatelům, kteří v současné době působí, nebo teprve mohou působit jako poskytovatelé Objednatele, a to zejména poskytovatelům, jejichž plnění souvisí s provedením integrace systémů dle této smlouvy, přičemž tak bude činit vždy ve lhůtě stanovené Objednatelem, která nesmí být kratší než 3 (tři) pracovní dny;
   5. dodržovat provozní řád v místě plnění a provádět svoje činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz na pracovištích Objednatele; Poskytovatel zajistí, aby všechny osoby, které se na jeho straně podílí na realizaci plnění a které budou přítomny v prostorách Objednatele, dodržovaly všechny bezpečnostní a provozní předpisy tak, jak s nimi byly seznámeny Objednatelem, nebo jak plynou z právních předpisů;
   6. informovat Objednatele na jeho žádost o průběhu realizace plnění;
   7. použít veškeré podklady předané mu Objednatelem pouze pro účely smlouvy a zabezpečit jejich řádné vrácení Objednateli, bude-li to objektivně možné vzhledem k jejich povaze a způsobu použití; Poskytovatel je povinen uvedené podklady vrátit Objednateli do čtrnácti dnů ode dne doručení výzvy Objednatele;
   8. zabezpečit účast pracovníků Poskytovatele či jím určených osob na pracovních schůzkách dle požadavků Objednatele sdělených alespoň tři pracovní dny předem.
2. Poskytovatel se dále zavazuje:
   1. uchovávat veškerou dokumentaci související s realizací Projektu IROP včetně účetních dokladů minimálně do konce roku 2031. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji Poskytovatel použít.
   2. Poskytovatel je povinen minimálně do konce roku 2030 poskytovat požadované informace a dokumentaci související s realizací Projektu IROP zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci Projektu IROP a poskytnout jim při provádění kontroly součinnost. Poskytovatel je povinen dodržovat aktuální Obecná a Specifická pravidla pro příjemce výzvy č. 23 IROP (ke stažení [https://www.irop.mm](http://www.irop.mmr.cz/cs/Vyzvy/Seznam/Vyzva-c-23-Specificke-)r.c[z/cs/Vyzvy/S](http://www.irop.mmr.cz/cs/Vyzvy/Seznam/Vyzva-c-23-Specificke-)eznam[/Vyzva-c-23-Specificke-](http://www.irop.mmr.cz/cs/Vyzvy/Seznam/Vyzva-c-23-Specificke-) informacni-a-komunikacni-sys).
3. Objednatel je oprávněn spolupracovat při provádění dohledu nad stavem provádění plnění s vybranou třetí osobou pro zajištění odborné garance na straně Objednatele. Poskytovatel je povinen plně respektovat postavení takové třetí osoby, a to pokud mu byl její výběr písemně oznámen Objednatelem, spolupracovat s ní a poskytnout jí maximální součinnost dle pokynů Objednatele.
4. Poskytovatel je povinen kdykoliv v průběhu trvání účinnosti smlouvy na vyzvání Objednatele prokázat, že disponuje dostatečnými kapacitami (realizačním, resp. pracovním týmem a jeho jednotlivými expertními členy, technickými zařízeními apod.) k provádění plnění dle této smlouvy a také je současně povinen prokázat, že řádně postupuje s plněním této smlouvy.

### XI.

### Ostatní ustanovení

1. Poskytovatel bere na vědomí, že podle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění, je povinen spolupůsobit při výkonu finanční kontroly. Tato povinnost se týká rovněž těch částí smlouvy a souvisejících dokumentů, které podléhají ochraně podle zvláštních právních předpisů (např. jako obchodní tajemství, utajované informace) za předpokladu, že budou splněny požadavky kladené právními předpisy (např. zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), v platném znění). Poskytovatel bere na vědomí, že obdobnou povinností je povinen smluvně zavázat také své poddodavatele. Povinnost dle tohoto odstavce trvá po dobu 10 let ode dne nabytí účinnosti této smlouvy.
2. Odstoupení od této smlouvy či jiné ukončení smluvního vztahu založeného touto smlouvou se nedotýká práva na zaplacení smluvní pokuty nebo úroku z prodlení, pokud již dospěl, práva na náhradu škody vzniklé z porušení smluvní povinnosti, ujednání o mlčenlivosti a ochraně informací ani ujednání, které má vzhledem ke své povaze zavazovat strany i po odstoupení od smlouvy, zejména ujednání o způsobu řešení sporů.
3. Poskytovatel může zajistit dodání Předmětu plnění prostřednictvím třetí osoby (poddodavatele) pouze na základě předchozího písemného souhlasu Objednatele. V případě, že je předmět plnění, či jakákoli jeho část plněna prostřednictvím třetí osoby, odpovídá Poskytovatel v takovém případě za plnění prováděná třetí osobou tak, jako by plnil sám.

### XII.

### Závěrečná ustanovení

1. Poskytovatel a Objednatel prohlašují, že jsou oprávněni uzavřít tuto smlouvu a že jim nejsou známy žádné právní a věcné překážky, které by bránily uzavření této smlouvy.
2. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv. Uveřejnění zajistí na své náklady Objednatel.
3. Otázky neupravené touto smlouvou se řídí českým právním řádem, zejména zákonem č. 89/2012, občanský zákoník, v platném znění. Strany se zavazují při realizaci smlouvy postupovat rovněž v souladu s Programovým dokumentem IROP, Prováděcím dokumentem IROP, dále v souladu s výzvou k předkládání žádostí o finanční podporu relevantní pro účel a předmět smlouvy včetně jejich veškerých příloh (dále také „Výzva“) a v souladu s příručkami, metodikami, oficiálními doporučeními, oznámeními a dalšími písemnými pokyny řídícího orgánu či zprostředkujícího subjektu dané Výzvy v aktuálním platném a účinném znění.
4. Případné spory z této smlouvy budou řešeny před věcně a místně příslušnými soudy České republiky.
5. Všechny přílohy této smlouvy tvoří její nedílnou součást. Smluvní strany sjednávají, že v případě jakéhokoliv rozporu mezi zněním této smlouvy a jejími přílohami má přednost znění této smlouvy.
6. Veškeré změny či doplňky této smlouvy musí být provedeny formou písemných vzestupně číslovaných dodatků.
7. Tato smlouva je vyhotovena ve dvou vyhotoveních, přičemž každá smluvní strana obdrží po jednom z nich.

*Přílohy:*

* + *Příloha č. 1 – Specifikace Díla a služeb*
  + *Příloha č. 2 – Napojené systémy*
  + *Příloha č. 3 – Položkový rozpočet*
  + *Příloha č. 4 – Návrh Poskytovatele*

V Klecanech dne V Brně dne

Objednatel Poskytovatel

**SPECIFIKACE DÍLA A SLUŽEB**

**veřejné zakázky Dodávka systému Identity managementu II.**

**Obsah**

1. [ÚČEL DOKUMENTU 3](#_TOC_250021)
2. [ZÁKLADNÍ INFORMACE 3](#_TOC_250020)

[INFORMACE O OBJEDNATELI 3](#_TOC_250019)

[CÍLE ZAKÁZKY 3](#_TOC_250018)

[INFORMACE O ZAKÁZCE 4](#_TOC_250017)

[PROSTŘEDÍ OBJEDNATELE 4](#_TOC_250016)

[TECHNOLOGICKÉ PROSTŘEDÍ OBJEDNATELE 5](#_TOC_250015)

[SOUVISEJÍCÍ ZAKÁZKY 5](#_TOC_250014)

1. [TECHNICKÁ SPECIFIKACE – DODÁVKA ŘEŠENÍ IDENTITY MANAGEMENTU 6](#_TOC_250013)

[ZÁKLADNÍ POŽADAVKY 6](#_TOC_250012)

[FUNKČNÍ POŽADAVKY 8](#_TOC_250011)

[TECHNICKÉ POŽADAVKY IDM 9](#_TOC_250010)

[DODRŽOVÁNÍ TECHNICKÉHO STANDARDU OBJEDNATELE 10](#_TOC_250009)

1. [POŽADAVKY NA DODÁVKU SLUŽEB 11](#_TOC_250008)

[PROVEDENÍ VSTUPNÍ ANALÝZY NAPOJENÝCH SYSTÉMŮ, TECHNOLOGIÍ APOD 11](#_TOC_250007)

[SLUŽBY IMPLEMENTACE IDM A ZAPOJENÍ DO ARCHITEKTURY NÚDZ 11](#_TOC_250006)

[NAPOJENÍ SYSTÉMŮ OBJEDNATELE 12](#_TOC_250005)

[ZPRACOVÁNÍ SOUVISEJÍCÍ DOKUMENTACE 12](#_TOC_250004)

[PROVEDENÍ MIGRACE NA NOVÝ HW 12](#_TOC_250003)

[POSKYTNUTÍ ZÁRUKY 13](#_TOC_250002)

[POSKYTNUTÍ PROVOZNÍ PODPORY V RÁMCI NEZPŮSOBILÝCH VÝDAJŮ PROJEKTU 14](#_TOC_250001)

[POSKYTNUTÍ SLUŽEB ROZVOJE SYSTÉMU 14](#_TOC_250000)

# Účel dokumentu

Tento dokument obsahuje specifikaci řešení a technických požadavků na systém Identity managementu (dále také jen jako „IdM“).

# Základní informace

## Informace o Objednateli

Národní ústav duševního zdraví (dále jen NUDZ) je státní příspěvkovou organizací v přímé řídící působnosti Ministerstva zdravotnictví a je samostatným právním subjektem se zaměřením na poskytování psychiatrické zdravotní péče, výzkumnou činnost a vzdělávání.

Oblast **zdravotní péče** je zajištěna psychiatrickou klinikou s lůžkovou a ambulantní částí, která poskytuje vysoce kvalitní diferenciálně diagnostickou a terapeutickou péči.

Mimo poskytování zdravotní péče je NUDZ **referenční výzkumné pracoviště** pro oblast duševního zdraví v České republice s mezinárodním dopadem. Zaměřením ústavu je výzkum neurobiologických mechanismů vedoucích k rozvoji nejzávažnějších duševních poruch (schizofrenie, poruchy nálady, úzkostné, spánkové a kognitivní poruchy). Součástí činnosti je rovněž vývoj a testování nových diagnostických a léčebných metod. Přístup k řešení problematiky je založený na vzájemné provázanosti metodik molekulární biologie, animálního modelování a klinického výzkumu a testování. V **oblasti pedagogické** je NUDZ klinickou základnou 3. lékařské fakulty Univerzity Karlovy a jako Klinika psychiatrie a lékařské psychologie 3. LF UK zajišťuje pregraduální a postgraduální vzdělávaní jak v oborech klinických (psychiatrie, psychologie), tak v oblasti neurověd. NUDZ poskytuje a zajišťuje vzdělávání pregraduální, postgraduální, specializační i vzdělávání cílené na soustavné rozvíjení znalosti a dovednosti výzkumníků.

NUDZ je v oblasti výzkumu příjemcem dotací a grantů z různých zdrojů (evropské fondy, Technologická agentura ČR, Grantová agentura ČR, soukromé zdroje). Týmy pro realizaci projektů z uvedených zdrojů financování jsou složeny z pracovníků různých profesí a specializací. Jednotlivé projekty pracují s odlišnými množinami pacientů nebo lidí z kontrolního vzorku. V rámci týmů mají pracovníci přístupová oprávnění k různým typům dat, přičemž jeden pracovník může mít díky účasti v různých týmech několik typů oprávnění k datům v různých systémech.

## Cíle zakázky

Cílem zakázky je vytvoření podmínek pro efektivní správu uživatelských identit a správu oprávnění pro systémy využívané Objednatelem a jejich moduly. S ohledem na výše uvedenou charakteristiku Objednatele je správa identit a uživatelských oprávnění jedním z klíčových faktorů při naplnění legislativních požadavků v oblasti bezpečnosti informací a ochrany dat, zejména s ohledem na snahu o elektronizaci procesů a zvýšení podílu elektronické dokumentace. Objednatel požaduje dodávku systému, který umožní správu přístupů nejen na úrovni aplikace a jejich modulů, ale zároveň i na úrovni skupiny dat (například jeden člen projektového týmu bude mít plný přístup k pacientským datům v příslušném systému, druhý člen bude mít v tomtéž systému přístup pouze k datům anonymizovaným).

## Informace o zakázce

**Projekt je financován z Evropského fondu pro regionální rozvoj, konkrétně z výzvy č. 23 - Specifické informační a komunikační systémy a infrastruktura I. Integrovaného regionálního operačního programu (IROP).** Poskytovatel tak bude při realizaci zakázky povinen dodržovat pravidla Výzvy.

## Prostředí Objednatele

Prostředí Objednatele zahrnuje (počty a procenta jsou přibližné, s možnou odchylkou až 20%):

* + fyzické osoby:
    - 600 zaměstnanců ve 100 různých pracovních pozicích (15 % zaměstnanců tvoří výzkumný zdravotnický personál, 75 % tvoří výzkumný nezdravotnický personál, 10

% podpůrný personál),

* + - 400 dohod o provedení práce/pracovní činnosti,
    - 100 aktuálně hospitalizovaných pacientů,
    - 300 subjektů účastnících se výzkumu,
    - 50 externistů/Poskytovatelů,
  + maticovou organizační strukturu, ze které zejména bude následně vyplývat požadavek na schopnost systému přiřazovat pracovníky do různých rolí:
    - pracovně-právní organizační strukturu tvoří 5 úseků, úseky se dále dělí na oddělení, ambulance nebo výzkumné programy, výzkumné programy (celkem 8) se dále dělí na pracovní skupiny (orientačně 5 pracovních skupin na výzkumný program),
    - projektová organizační struktura – dominantní část činnosti Objednatele se odehrává formou realizace projektů/grantů od různých poskytovatelů (běžně řešených projektů/grantů může být 100 a více, současný počet je cca 80), každý grant má hlavního řešitele a další řešitele, kteří mohou být ke grantu přiřazeni nezávisle na výše uvedené organizační struktuře,
    - vnitřní kontrolní systém – Objednatel hospodaří s veřejnými prostředky a podléhá působnosti zákona č. 320/2001 Sb., o finanční kontrole, v platném znění včetně prováděcích právních předpisů, má tedy zaveden vnitřní kontrolní systém a pro schvalování finančních závazků a nároků má určeny role příkazce operace, správce rozpočtu, hlavní účetní, a dále například roli administrátor grantu a jejich zástupce (tyto role jsou určeny ke každému zdroji financování, což jsou zejména jednotlivé projekty/granty – viz výše; v některých grantech vystupuje Objednatel jako spoluřešitel spolu s jinými organizacemi),
    - Objednatel má zřízeno zhruba 10 komisí s trvale jmenovanými členy.
  + systém elektronické kontroly vstupu do různých částí budovy:
    - počet aktivních karet 750,
    - počet čteček/ovládaných dveří 100,
    - počet úrovní přístupů zahrnující vybranou čtečku/dveře 100,
    - každé kartě může být přiřazena pro přístup jedna hlavní úroveň přístupu, jedna vedlejší úroveň přístupu a jedna další konkrétní čtečka/dveře.

## Technologické prostředí Objednatele

Technologické prostředí Objednatele zahrnuje:

1. Jednotnou centrální adresářovou (a ověřovací) službu na platformě Active Directory (1 forest, 2 domény, doménové kontroléry verze Windows Server 2012 R2), integrované a centrálně spravované pracovní stanice a servery Objednatele na platformě Windows i Linux.
2. Informační systémy, aplikace a služby integrované do prostředí Active Directory (např. Microsoft Exchange 2016, Microsoft Certificate Authority) – snahou Objednatele je v rozumné míře integrovat SSO ověřování s využitím identitních a ověřovacích prostředků Active Directory – u nativních Windows aplikací pomocí Integrated Windows Authentication, v prostředí Linuxu pak využití LDAP/Kerberos.
3. SSO webový portál (SSO webový portál organizace pro webový přístup) formou integrace na stávající SSO portál objednatele protokolem SAML 2.0 (SW Shibboleth Identity Provider 4), který ověřuje uživatele vůči Active Directory – snahou Objednatele je v rozumné míře implementovat SSO ověřování u webových a cloudových aplikací vůči SSO webovému portálu.
4. Různé informační systémy, které nejsou nativně integrované do Active Directory – využívají zabudovaný autorizační profil uživatele a/nebo lokální autentizaci resp. využivají složitější systém přístupových práv a které Objednatel zamýšlí řídít pomocí IdM.
5. Workflow a formulářovou komponentu, která obsahuje centrální místo - elektronickou podpisovou knihu - jako nástroj pro centrální schvalování libovolných dokumentů; jedná se o informační systém, který je předmětem jiné veřejné zakázky.

Prostředí Objednatele resp. informační systémy, které Objednatel vyžaduje integrovat jako součást plnění, jsou popsané v Příloze č. 2 Smlouvy. Objednatel upozorňuje, že integrační vazby popsané a znázorněné Příloze č. 2 popisují pouze klíčové vazby a zdroje referenčních dat a nejedná se o kompletní popis všech požadovaných integračních vazeb a všech zdrojů referenčních dat – ty budou předmětem návrhu implementace schváleného odpovědnými pracovníky zadavatele .

## Související zakázky

V rámci projektu, ze kterého je financováno pořízení systému pro správu identit, jsou realizovány i další projekty, které slouží k rozvoji elektronické formy komunikace a zavedení principů eHealth. Z tohoto důvodu bude napojování aplikací do IdM probíhat postupně, po celou dobu realizace projektu.

1. Technická specifikace – dodávka řešení Identity managementu

V této kapitole je uvedena ucelená množina požadavků, které jsou kladeny na nástroj Identity managementu (dále jen „IdM“ nebo „Systém“).

## Základní požadavky

|  |  |
| --- | --- |
| **Číslo**  **požadavku** | **Popis požadavku** |
| 1.1 | IdM umožňuje v adresářové službě a řízených informačních systémech Objednatele synchronizaci lidí včetně jejich přístupových účtů a hesel tj. zejména zaměstnanců/dohod o provedení práce/pracovní činnosti, externistů, pacientů a subjektů výzkumu (nástup/ukončení zaměstnance/ externisty/pacienta/subjektu  výzkumu, změna pracovní pozice/hospitalizace atd.). |
| 1.2 | IdM umožňuje v adresářové službě a řízených informačních systémech Objednatele synchronizaci organizačních útvarů a skupin (dominantní část činnosti Objednatele se odehrává formou realizace projektů/grantů, použitý systém uživatelských práv/rolí tedy musí bezpodmínečně respektovat několik rovin práv/rolí:   1. v **organizační rovině** v souladu zejména s Organizačním řádem Objednatele (organizační útvary, zařazení zaměstnanců do nich, vztahy nadřízenosti a podřízenosti), 2. v **rovině finančních zdrojů** v souladu s Vnitřním kontrolním systémem Objednatele (typicky příkazce operace, správce rozpočtu, apod.), 3. v **rovině odpovědné osoby** (např. za místnost v případě evidence majektu, osoby, která majetek převzala apod.), 4. v **rovině ustanovené komise** (např. personální nebo likvidační) tj. specifických   skupin s trvale jmenovanými členy, |
| 1.3 | IdM umožňuje v adresářové službě a řízených informačních systémech Objednatele synchronizaci servisních účtů (pro vnitřní potřebu IT systémů) a externistů (např.  Poskytovatelé provádějící dočasné či průběžné servisní práce, dočasné stáže). |
| 1.4 | IdM umožňuje v adresářové službě a řízených informačních systémech Objednatele  synchronizaci přístupových karet a fyzických přístupových úrovní v systému elektronické kontroly vstupu (ACS). |
| 1.5 | Systém umožňuje tvorbu, synchronizaci, řízení, blokování a mazání identit, rolí a dalších potřebných objektů v centrální adresářové službě a informačních systémech  řízených nástrojem IdM. |
| 1.6 | Systém podporuje rozdílovou i celkovou synchronizaci změn do/z řízených  informačních systémů a adresářové služby. |
| 1.7 | Systém umožňuje přebírání zdrojových dat, publikace a změny dat z různých referenčních zdrojů ve stávajících, modernizovaných a nově pořizovaných informačních systémech včetně případného vytvoření integračního rozhraní na straně nástroje ve spolupráci s jejich dodavateli/výrobci, zejména:   1. interní systém organizace pro řízení lidských zdrojů = referenční zdroj zdravotnických a nezdravotnických pracovníků organizace a pracovně-právní organizační struktury 2. interní nemocniční informační systém organizace = referenční zdroj pacientů,   resp. subjektů účastnících se výzkumu, |

|  |  |
| --- | --- |
|  | 1. interní informační systém pro evidenci grantů = referenční zdroj řešitelů a projektů (projektová organizační struktura), 2. nástroj pro správu životního cyklu kvalifikovaných certifikátů a prostředků pro vytváření kvalifikovaných elektronických podpisů dle eIDAS = referenční zdroj identifikátorů bezkontaktních čipových karet   Konkrétní způsob vzájemného předávání a správy referenčních dat mezi systémy budou předmětem návrhu implementace schváleného odpovědnými pracovníky  zadavatele. |
| 1.8 | IdM může být referenčním zdrojem dat (např. uživatelských účtů, evidence a přiřazení jednotlivých rolí v rovině finančních zdrojů pro konkrétní zdroje financování, evidenci souhlasů s veřejným použitím fotografie osoby, evidence komisí a jejich členů,  evidenci externích osob, dodavatelů a servisních účtů). |
| 1.9 | Systém umožňuje vytvoření uživatelského účtu včetně vygenerování počátečního hesla s vynucením jeho změny při prvním použití po založení uživatele v referenčním zdroji (např. předání přihlašovacích údajů zaměstnanci na personálním oddělení v rámci  nástupu do zaměstnání). |
| 1.10 | Systém umožňuje provoz samoobslužného portálu pro obnovu zapomenutého hesla. |
| 1.11 | IdM bude poskytovat možnost zadání údajů pro samoregistrující uživatele. |
| 1.12 | IdM bude otevřený pro integrace na jiné budoucí datové základny. |
| 1.13 | Systém umožní správu rolí (RBAC) a průnik vícenásobných rolí (různé úvazky v různých odděleních/účast na různých grantech) včetně možnosti samoobslužné žádosti o určitou roli, řešení expirace a prodlužování přístupu (např. u ručně zakládaných  externistů). |
| 1.14 | IdM podporuje neomezenou hiearchii rolí včetně možnosti tvorby katalogu rolí a  podpora řízení životního cyklu rolí. |
| 1.15 | IdM podporuje možnost provádění inventury přístupových práv k zábranění  kumulování většího množství práv jedné osoby v průběhu času včetně vynuceného přeschválení rolí s eskalačním mechanismem. |
| 1.16 | IdM poskytuje podporu principu „čtyř očí“, tedy je možné kontrolovat, že osoba s přidělenou specifickou rolí nemůže mít zároveň přidělena jinou specifickou roli (např. příkazce operace a správce rozpočtu stejného zdroje financování v rámci vnitřního  kontrolního systému nemůže být tatáž osoba). |
| 1.17 | IdM obsahuje podporu kontrolních mechanismů na byznys vrstvě, která umožní  sledovat chybějící oprávnění (např. příkazce operace finančního zdroje ukončí pracovní poměr a bez nominace jiného příkazce operace nelze finační zdroj čerpat). |
| 1.18 | IdM umožňuje vytváření více typů účtů (více uživatelských jme, resp. identit) k jedné  fyzické osobě (např. běžný a administrátorský účet). IdM bere tento fakt v potaz. |
| 1.19 | IdM umožňuje reporting a vytváření auditní stopy operací nad činností IdM a  oprávněných uživatelů (historické změny v uživatelských účtech, historické změny v uživatelských rolí, schvalování apod.). |
| 1.20 | IdM spravuje identity v řízených informačních systémech prostřednictvím vlastních konektorů, které jsou využívány rozhraním daného systému (např. CSV, ODBC, LDAP, REST, SOAP apod.) bez nutnosti instalace pomocné komponenty (agenta) do řízeného informačního systému/adresářové služby; kromě plně automatizovaných konektorů (čtení/zápis do/z informačního systému) IdM podporuje plně manuální  konektor (notifikuje odpovědné osoby o nutnosti ruční změny v informačním systému) |

|  |  |
| --- | --- |
|  | a poloautomatický konektor (notifikuje odpovědné osoby o nutnosti ruční změny, ale  zároveň umožňuje manuální načtení stavu v informačním systému pro kontrolu). |
| 1.21 | Webové rozhraní pro žádost o přidělení práv prostřednictvím IdM má ovládání přizpůsobené různým dotykovým zařízením (responzivní design pro samoobslužnou část) a platformám (iOS, Android atd.), přístup do klientské části je nezávislý na operačním systému přistupujícího klienta a možný prostřednictvím webového prohlížeče bez nutnosti instalace dalšího SW (aplikací, modulů, appletů či knihoven)  tj. zejména bez použití např. ORACLE Java, Microsoft Silverlight, Adobe Flash. |
| 1.22 | Autentizace/autorizace uživatelů k webovému rozhraní IdM bude připraveno na využití  SSO webového portálu. |
| 1.23 | Systém musí být připraven na napojení na Národní identitní autoritu. |

## Funkční požadavky

|  |  |
| --- | --- |
| **Číslo**  **požadavku** | **Popis požadavku** |
| 2.1 | IdM disponuje záznamem vybraných operací nad identitami v auditním logu, přičemž  historie změn bude zahrnovat i autora změny. |
| 2.2 | Systém obsahuje profily uživatelů, k nimž jsou přiřazována příslušná oprávnění. |
| 2.3 | Systém umožňuje vícekriteriální vyhledávání a ukládání filtrů. |
| 2.4 | Systém umožňuje omezení přístupů uživatelů do různých částí evidovaných dat. |
| 2.5 | Systém umožňuje přenášení oprávnění z osoby na osobu (jeden uživatel bude dělat  totéž, co předchozí). |
| 2.6 | Systém umožňuje kopírování oprávnění mezi prostředími (produkční a testovací). |
| 2.7 | Systém udržuje historii provedených změn u pracovníků s možností zobrazení stavu ve vybraném čase (podle data je možné ukázat, jaké bylo nastavení k příslušnému datu),  které musí být shodné se standardním zobrazením dat. |
| 2.8 | Systém uchovává informace o odstraněných pracovnících (neaktivní účty s posledním  platným nastavením). |
| 2.9 | IdM musí umožnit reagovat na události změny organizační struktury, změny oprávnění  nebo změny vlastností identit tak, že odešle relevantní informaci formou e-mailu. Konfigurace událostí a reakcí na ně musí být uživatelsky definovatelné. |
| 2.10 | Systém umožňuje provádění kontroly konzistence dat skutečného stavu v adresářové službě a řízených informačních systémech oproti očekávanému stavu v IdM (zejména kvůli odhalení změn, které byly do adresářové služby nebo řízených informačních  systémů zaneseny mimo IdM např. ručním zásahem administrátora). |
| 2.11 | Systém podporuje mapování atributů mezi různými řízenými informačními systémy a adresářovou službou – převod hodnot mezi různými atributy včetně možnosti algoritmizovat způsob převodu pomocí transformační logiky/skriptovacího jazyka (např. slučování/rozdělování atributů do jednoho/více atributů, textové úpravy hodnot, odstranění diakritiky, definici podmínek včetně absolutního a relativního času – např.  smazání účtu až po x dnech od ukončení pracovního poměru/zablokování) |
| 2.12 | Systém zahrnuje uživatelské rozhraní pro manuální editaci vybraných informací z  uživatelského profilu, např. uživatelské heslo. |

|  |  |
| --- | --- |
| 2.13 | Systém umožňuje jednotnou evidenci maticové organizační struktury (organizační –  pracovně-právní a projektové/grantové). |
| 2.14 | V systému lze provádět nastavení přístupových práv do aplikací s využitím profilů, a  přístupových práv k datům na souborovém systému v prostředí Windows. |
| 2.15 | Systém umí generovat výstupy pro podporu tvorby telefonního seznamu organizace ve formě webových služeb, exporty dat do XML, grafické znázornění organigramu  organizace. |
| 2.16 | Systém odesílá e-mailovou notifikaci definované osoby v případě vytvoření, přesunutí  nebo odstranění. |
| 2.17 | Systém odesílá e-mailovou notifikaci zastupující osobě v případě vytvoření zástupu. |
| 2.18 | Systém poskytne rozhraní pro import uživatelských rolí z integrovaných systémů. |
| 2.19 | Systém umožní evidenci uživatelů, kteří nebudou synchronizováni do centrální  adresářové služby. |
| 2.20 | Systém musí umožnit evidenci všech aplikací provozovaných v organizaci, a to až na  úroveň jednotlivých modulů. |
| 2.21 | Systém umožní fulltextové vyhledávání v aplikaci pro vybrané vlastnosti evidovaných  objektů. |
| 2.22 | Systém umožní filtrování v seznamech (seznam aplikací, seznam osob, seznam  organizačních jednotek apod.). |

## Technické požadavky IdM

Nástroj IdM bude splňovat následující technické požadavky.

|  |  |
| --- | --- |
| **Číslo**  **požadavku** | **Popis požadavku** |
| 3.1 | GUI Systému podporuje aktuální verze prohlížečů:   * Microsoft Internet Explorer * Microsoft Edge * Google Chrome (desktop, Android) * Mozilla Firefox * Safari pro iOS/iPadOS |
| 3.2 | Systém bude obsahovat nápovědu přímo v aplikaci (formulářová a položková  nápověda). |
| 3.3 | Součástí dodávky IdM je kompletní uživatelská a administrátorská dokumentace  v elektronické verzi. |
| 3.4 | IdM bude obsahovat obecné zdokumentované rozhraní pro vstup dat z personálního systému včetně importu nadřízenosti a podřízenosti jednotlivých rolí, budov organizace  a kontaktů pracovníků (telefonní čísla, e-maily, místnosti). |
| 3.5 | Objednatel požaduje poskytnutí zdrojového kódu ke konektorům a programovým  úpravám, které byly v rámci dodávky vytvořeny/upraveny pro potřeby Objednatele. |

## Dodržování technického standardu Objednatele

Všechny nabízené komponenty informačního systému musí být provozovány ve stávajícím serverovém virtualizačním prostředí objednatele (VMware vSphere 6.x).

Pro jakýkoli webový přístup k aplikaci je povinně vyžadováno zabezpečení komunikace pomocí TLS (HTTPS) včetně automatického přesměrování z nezabezpečené komunikace (HTTP), potřebný TLS certifikát poskytne objednatel.

Všechny nabízené komponenty informačního systému musí podporovat přístup internetovým protokolem verze 4 (IPv4) i internetovým protokolem verze 6 (IPv6).

Objednatel nabízí k využití následující komponenty v uvedené kapacitě stávajícího výpočetního prostředí:

1. Hardware, resp. dostupný volný výkon:
   * operační paměť (RAM): cca 32 GB a současně dostatečná rezerva 32 GB virtuální RAM na případné rozšíření,
   * procesor (CPU): přiděleny mohou být maximálně 4 jádra procesoru Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz na jeden virtuální server, celkem až 4 volné virtuální servery,
   * diskové pole: aktuálně dostupné cca 1 TB na discích typu SAS 10k a 2 TB na discích typu SAS 7k2.
2. databáze: Microsoft SQL Server 2016 Standard na virtuálním serveru (4xvCPU 16GB RAM) s aktuální zátěží v míře cca 20% dostupného výkonu.
3. licence operačního systému: Microsoft Windows 2012 R2 Server Standard

Pokud uchazeč pro běh systému navrženého ve své řešení bude vyžadovat jiné komponenty třetích stran nebo jejich jiné verze, požadujeme takové součásti zahrnout do nabídky, tj. do návrhu řešení (licence musí umožňovat neomezenou živou migraci ve stávajícím virtualizačním prostředí) a nabídkové ceny, a explicitně je popsat samostatně v nabídce.

1. Požadavky na dodávku služeb

V rámci dodávky bude Poskytovatel odpovědný za realizaci níže uvedených činností, které jsou nedílnou součástí celého projektu. Poskytovatel se zavazuje poskytnout NUDZ služby, spočívající v komplexní realizaci Díla, tak jak byl jeho předmět vymezen v Zadávací dokumentaci včetně všech jejích příloh, smlouvě a této příloze č. 1 smlouvy (není-li dále stanoveno jinak). Tyto služby zahrnují zejména (nikoliv výlučně):

## Provedení vstupní analýzy napojených systémů, technologií apod.

Poskytovatel zpracuje úvodní analýzu používaných systémů a technologií, která zahrnuje minimálně:

1. **Analýzu požadavků**
   1. Provedení technické analýzy systémů a evidencí napojených do IdM.
   2. Analýza požadavků na bezpečnost systémů a požadavků na jejich provoz.
   3. Provedení analýzy organizačních aspektů souvisejících se správou a provozem systémů a analýza životního cyklu uživatelských identit a návrh způsobu jejich naplnění.
2. **Návrh, projednání a schválení implementace**

Na základě analýzy bude vytvořen návrh implementace. Součástí tohoto návrhu bude návrh uživatelského rozhraní, návrh zapojení jednotlivých systémů, návrh způsobu řízení přístupových oprávnění v celém životním cyklu, návrh akceptačních procedur a testování předcházejících předání a akceptaci napojení jednotlivých systémů před spuštěním produktivního provozu. Součástí návrhu implementace budou veškeré další informace a postupy nutné pro úspěšnou implementaci systému pro správu identit.

1. **Stanovení požadavků na součinnost Poskytovatelů zapojených systémů**

Jedním z výstupů úvodní analýzy bude návrh požadavků na součinnost dodavatelů zapojených systémů, na jejichž základě Objednatel dle svých možností pokusí požadovanou součinnost zajistit. V případě, že se tuto součinnost zajistit nepodaří, předloží Poskytovatel v příslušných bodech návrh požadavků na součinnost dodavatelů zapojených systémů, která bude nezbytná pro splnění povinností Poskytovatele dle smlouvy. Na základě uvedených požadavků Objednatel požadovanou součinnost zajistí.

## Služby implementace IdM a zapojení do architektury NÚDZ

Na základě konsenzuální podoby návrhu implementace, schváleného odpovědnými pracovníky Objednatele, bude provedena implementace IdM. Implementace bude zahrnovat:

* 1. Instalaci IdM na poskytnutý HW a zpřístupnění systému vybraným pracovníkům

Objednatele, kteří se budou podílet na správě systému.

* 1. Úpravy řešení dodaného systému tak, aby plně odpovídal požadavkům zadání.
  2. Nastavení životního cyklu uživatelských identit a přístupových oprávnění a napojení na systémy, které s identitami pracují (personální systém, AD apod.).
  3. Testování systému
     1. Provedení funkčních testů;
     2. Provedení bezpečnostních testů;
     3. Vyhodnocení testování a realizace opatření z testování vyplývajících.
  4. Školení administrátorů systému (3 osoby).

## Napojení systémů Objednatele

Poskytovatel provede napojení všech požadovaných mandatorních informačních systémů, uvedených v kapitole 1 Přílohy č. 2 Smlouvy – Spolupracující systémy, na systém IdM. Napojení bude prováděno průběžně podle toho, jak budou jednotlivé systémy pořizovány, případně rozvíjeny. Objednatel stanoví, že napojení může být realizováno od druhého čtvrtletí roku 2021 podle toho, jak budou dokončovány implementace jednotlivých systémů.

Objednatel předpokládá, že součinnost potřebná od dodavatelů uvedených systémů, plánovaných k napojení do IdM, bude vyžádána v rámci samostatných smluvních vztahů mimo předmět této zakázky. Napojení ostatních systémů, které jsou uvedeny v Příloze č. 2 Smlouvy jako nepovinné, bude Objednatel realizovat prostřednictvím dílčích objednávek na základě sazby za člověkohodinu, stejně jako potřebu dalších prací rozvoje.

Součástí Díla je úvodní konfigurace přístupových oprávnění do jednotlivých systémů na základě vstupních údajů poskytnutých Objednatelem.

## Zpracování související dokumentace

Součástí dodávky bude zpracování veškeré související dokumentace, která bude nutná pro obsluhu systému. Součástí dodávky bude technická, administrátorská i uživatelská dokumentace.

1. **Zpracování technické dokumentace systému**
   1. Zpracování dokumentace aplikací.
   2. Dokumentace reálného nasazení - popis technologické infrastruktury - analytické dokumenty odpovídající reálnému nasazení systému;
2. **Zpracování provozní dokumentace**
   1. Uživatelské manuály pro všechny role v systému,
   2. Provozní řád systému, který upravuje chování jeho uživatelů,
   3. Servisní řád upravující poskytování provozní podpory mezi NÚDZ a Poskytovatelem,
   4. Bezpečnostní dokumentace

## Provedení migrace na nový HW

Součástí dodaných služeb bude i provedení migrace dodaného systému a všech jeho součástí na nový HW, který bude pořízen v rámci stejného dotačního projektu, a to včetně konfigurace pro všechny napojené systémy, které budou migrovány též. Poskytovatel se zavazuje poskytnout podporu při migraci a provést všechny nezbytné úpravy tak, aby byla zajištěna bezproblémová migrace celého poskytovatelem dodaného řešení do nového prostředí, tedy nejen samotného nástroje IdM. Migrace na nový HW bude realizována ve třetím čtvrtletí roku 2021.

## Poskytnutí záruky

Poskytovatel poskytuje na předmět plnění dle smlouvy záruku na dobu 60 měsíců. Poskytovatel bude za účelem řešení záručních vad garantovat, vyjma samotného odstranění vady, také následující služby:

* Služba HelpDesk minimálně v následujícím rozsahu:
  + Webové rozhraní nebo e-mailová adresa pro zajištění veškeré písemné komunikace a řešení technických problémů pro administrátory s možností sledovat stav požadavku,
  + Rozhraní pro řešení vad, vznesení metodických, uživatelských a dalších dotazů souvisejících se záručními vadami,
  + Dostupnost minimálně 10 hodin x 5 dní v týdnu (pracovní dny 8:00 – 18:00 hod.).
* Vzdálená správa – slouží k řešení vad, k úpravě konfigurace a podobně. Vzdálená správa není určena ke školení a metodickému vedení. Objednatel zajistí vzdálený přístup (VPN) pro Poskytovatele v potřebném rozsahu tak, aby mu byl umožněn přístup na server(y), kde je umístěna testovací, školící a produkční verze Systému.

Klasifikace záručních zásahů a doby řešení:

**Kategorie A** – priorita „Critical“ je kritická vada, kdy práce se Systémem není vůbec možná, v důsledku čehož nelze vůbec realizovat klíčové procesy Objednatele v rámci Informačního systému - např. nelze se přihlásit, uživatelské rozhraní nereaguje, není možný ani omezený provoz.

**Kategorie B** – priorita „Major“ je vážná vada, kdy práce se Systémem je zásadním způsobem omezena, v důsledku čehož lze realizovat pouze některé klíčové procesy Objednatele v rámci Systému. Za odstranění vady se považuje i nalezení náhradního postupu, nebo řešení, které zajistí funkčnost minimálně ve stejné úrovni.

**Kategorie C** – priorita „Minor“ je drobná vada, kdy práce se Systémem je omezena, v důsledku čehož lze realizovat některé klíčové procesy Objednatele v rámci Systému pouze s určitými obtížemi.

**Kategorie D** – priorita „Info“ je nevýznamná vada, kdy práce se Systémem není omezena a nemá dopad do funkčnost Systému – jedná se například o jazykové opravy, chyby v dokumentaci.

Reakční doby na zahájení opravy a odstranění závady definují následující tabulky: Provozní prostředí:

|  |  |  |
| --- | --- | --- |
| **Kategorie** | **Doba odezvy (od nahlášení)** | **Lhůta k vyřešení (od nahlášení)** |
| A | 4 hodiny | 24 hodin |
| B | 8 hodin | 72 hodin |
| C | 8 hodin | 120 hodin |
| D | 8 hodin | 168 hodin |

Testovací prostředí:

|  |  |  |
| --- | --- | --- |
| **Kategorie** | **Doba odezvy (od nahlášení)** | **Lhůta k vyřešení (od nahlášení)** |
| A | 8 hodin | 72 hodin |
| B | 1 pracovní den | 120 hodin |
| C | 2 pracovní dny | 168 hodin |
| D | 2 pracovní dny | 240 hodin |

Výše uvedené garantované lhůty jsou nejvýše přípustné a vztahují se k běžné pracovní době, a to od 8:00 do 18:00 hodin v pracovní dny, tj. vyjma svátků a dnů pracovního klidu oficiálně uznaných na území ČR apod., tzn., pokud přijde hlášení po uplynutí běžné pracovní doby, lhůta začíná běžet od začátku běžné pracovní doby následujícího pracovního dne, případně se její běh přerušuje a dokončí se během následujícího pracovního dne.

## Poskytnutí provozní podpory v rámci nezpůsobilých výdajů projektu

Přestože je poskytnutí maintenance a supportu v rámci 23. výzvy nezpůsobilým výdajem, je nedílnou součástí celkových nákladů poskytnutého řešení. Poskytovatel tak bude v rámci servisu poskytovat následující služby maintenance a supportu:

1. Maintenance zahrnuje následující plnění Poskytovatele:
   1. Dodávku nových verzí IdM (update a upgrade) včetně aktualizované dokumentace (uživatelské příručky, administrátorské příručky);
   2. Dodávku meziverzí či hotfix IdM s přehledem úprav, a to pokud budou tyto vyvolány zásahem třetího subjektu, kdy v případě že jde o meziverze či hotfix vyvolané samotnou činností Poskytovatele, spadají tyto do záručního plnění dle bodu č. 4.6 této přílohy;
   3. Poskytnutí oprav a patchů, které nespadají do záručních oprav dle bodu č. 4.6. této přílohy.
2. Support zahrnuje poskytnutí následujících činností Poskytovatele:
3. Řešení problémů s provozem IdM, používání telefonické podpory formou Hotline, a to u problémů, které nejsou kryty zárukou;
4. Rozhraní pro řešení vad, vznesení metodických, uživatelských a dalších dotazů, a to vždy když tyto vady, dotazy a pod nejsou kryty zárukou, resp. netýkají se problému krytého zárukou.
5. Činnosti jsou poskytovány nejen pro poslední uvolněnou verzi IdM, ale i o max. dvě verze nižší.
6. Hot-line v pracovní dny 8:00 – 18:00 hod
7. 1x ročně školení pro 2 administrátory systému v délce trvání 4 hodin po celou dobu trvání smlouvy

Uvedené činnosti budou poskytovány:

1. Vzdáleným připojením k serveru, na němž je nainstalován systém IdM;
2. Osobní přítomností pracovníků Poskytovatele v sídle zadavatele (pouze v případě, pokud nelze použít vzdálený přístup);
3. Telefonickou konzultací (HotLine) a prostřednictvím systému Help Desk zadavatele v požadované dostupnosti 5x10 hodin v pracovní dny.

Podpora poptávaného řešení je požadována po dobu 60 měsíců. Zahájení služeb podpory je ode dne termínu akceptace díla ve smyslu čl. III odst. 4 písm. a) Smlouvy .

## Poskytnutí služeb rozvoje Systému

Poskytovatel poskytne Objednateli konzultační a programátorské služby v celkovém rozsahu 400 člověkohodin a to jak v průběhu implementace Systému, tak i po termínu akceptace díla ve smyslu čl. III odst. 4 písm. a) Smlouvy do termínu nejméně 31. 10. 2026. Předmětem služeb jsou implementační, integrační a rozvojové požadavky nad rámec požadavků uvedených v této Příloze č. 1 Smlouvy, a to

zejména v oblasti napojení dalších systémů, uvedených v Příloze č. 2 jako nemandatorní. Tyto služby budou čerpány na základě vzájemně odsouhlasených dílčích písemných objednávek.

**NAPOJENÉ SYSTÉMY**

**veřejné zakázky Dodávka systému Identity managementu II.**

**Obsah**

**SYSTÉMY NAPOJENÉ JAKO MANDATORNÍ SOUČÁST REALIZACE ZAKÁZKY** **2**

**PERSONÁLNÍ A MZDOVÝ SYSTÉM – PAM** **2**

**MICROSOFT EXCHANGE** **2**

**ACTIVE DIRECTORY** **3**

**SPRÁVA ZAMĚSTNANECKÝCH KARET A KVALIFIKOVANÝCH CERTIFIKÁTŮ 3**

Tento dokument definuje informační systémy, jejichž napojení je součástí ceny veřejné zakázky a budou relizovány v rámci dodávky a implementace IdM, popisuje očekávaný způsob práce

s jednotlivými informačními systémy a centrální adresářovou službou.

**Systémy napojené jako mandatorní součást realizace zakázky**

Systémy uvedené v této kapitole jsou součástí dodávky systému a náklady na napojení uvedených systémů je součástí ceny Díla v souladu s ustanoveními Přílohy č. 1 Smlouvy Specifikace Díla a služeb.

Personální a mzdový systém – PaM

|  |  |
| --- | --- |
| **Autor/dodavatel systému,**  **produktové označení** | Personální a mzdový systém VEMA Mzdy od společnosti Vema,  a.s. |
| **Očekávání Zadavatele od napojení na IdM** | Referenční zdroj:   * osob (částečný) – zaměstnanců a osob s dohodami (DPP/DPČ) * pracovních pozic * pracovně-právní organizační struktury (vedoucí útvarů, vztahy nadřízenosti a podřízenosti útvarů) |
| **Charakteristika systému, způsob práce se systémem** | Personální a mzdový systém je primárním systémem Zadavatele pro evidenci osob s pracovně-právním vztahem vůči Zadavateli, dále slouží pro zpracování platů a odvodů vůči státu. Personalistická část pak slouží zejména k podpoře výběrových řízení, správu životního cyklu systemizovaných pracovních míst a organizační struktury a evidenci pracovní doby. **Tento systém je tedy klíčovým zdrojem rolí/práv v organizační rovině.** |
| **Očekávané rozhraní, způsob komunikace** | Očekává se automatizovaná komunikace, PaM systém poskytuje exporty dat ve formě sestav prostřednictvím CSV souborů, přičemž CSV soubory obsahují vždy celou datovou sadu (nelze vyžádat např. rozdílovou sadu od poslední synchronizace). Export aktuálních dat do CSV souboru lze vyžádat neinteraktivně z příkazové řádky z prostředí, kde je nainstalován PaM klient (pouze pro Windows platformu) případně je možné naplánovat pravidelný export a výstupy ukládat na smluvené místo na sdíleném disku přístupném protokolem CIFS nebo NFS  3.x/4.x. |

Microsoft Exchange

|  |  |
| --- | --- |
| **Autor/dodavatel systému,**  **produktové označení** | Microsoft Exchange 2016 |
| **Očekávání Zadavatele od**  **napojení na IdM** | Refereční zdroj:   * e-mailové adresy |

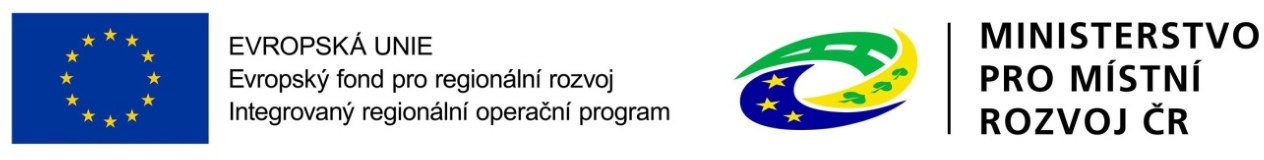
|  |  |
| --- | --- |
|  | Zadavatel očekává správu e-mailových schránek (vytváření,  rušení, správu e-mailových aliasů) v prostředí jedné Exchange organizace (2 servery). |
| **Charakteristika systému,**  **způsob práce se systémem** | Provoz e-mailového serveru Zadavatele. |
| **Očekávané rozhraní, způsob**  **komunikace** | Např. PowerShell, automatizovaná. |

Active Directory

|  |  |
| --- | --- |
| **Autor/dodavatel systému,**  **produktové označení** | Microsoft Active Directory (Windows Server 2012 R2) |
| **Očekávání Zadavatele od napojení na IdM** | Referenční zdroj:   * identifikátorů bezkontaktních přístupových karet * fotografií osob   Zadavatel očekává správu veškerých účtů, skupin a distribučních listů v prostředí dvou domén, které jsou součástí jednoho forestu. |
| **Charakteristika systému,**  **způsob práce se systémem** | Jednotná centrální adresářová (a ověřovací) služba. |
| **Očekávané rozhraní, způsob**  **komunikace** | Např. LDAP nebo PowerShell, automatizovaná. |

Správa zaměstnaneckých karet a kvalifikovaných certifikátů

|  |  |
| --- | --- |
| **Autor/dodavatel systému,**  **produktové označení** | Monet+ / CMS |
| **Očekávání Zadavatele od napojení na IdM** | Referenční zdroj:   * Čísla přidělených čipových karet a platnost certifikátů, vazba na data z EKV   Zadavatel očekává správu a přenos osob, údajů o platnosti  certifikátů |
| **Charakteristika systému, způsob práce se systémem** | Systém spravuje část přístupových čipových karet těch zaměstnanců, kteří disponují zároveň i zaručeným  kvalifikovaným ověřeným certifikátem/podpisem. |
| **Očekávané rozhraní, způsob komunikace** | Automatizovaně:  Čtení dat přímo z DBMS Microsoft SQL Server 2016 Standard běžící v operačním systému Microsoft Windows Server 2012 R2. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Položkový rozpočet - celkové náklady na vlastnictví systému (TCO)** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Dodavatel vyplní pouze žlutě označená pole** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Dodavatel přidá řádky pro detailní specifikaci ceny |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | **Náklady před spuštěním do rutinního provozu** | | | |  | **Náklady po finální akceptaci celého díla** | | |  |  |  |  |  |  |  |  |  |  |
| **Položka** | **Kalkulační jednotka (např. jádro, uživatel, rok, člověkoden, apod.)** | **Jednotková cena (bez DPH)** | **Jednotková cena (vč. DPH)** | **Počet jednotek** | **Náklady celkem (bez DPH)** |  | **Počet jednotek** | **Náklady na 1. rok provozu po finální akceptaci (bez**  **DPH)** | **Počet jednotek** | **Náklady na 2. rok provozu (bez DPH)** | **Počet jednotek** | **Náklady na 3. rok provozu (bez DPH)** | **Počet jednotek** | **Náklady na 4. rok provozu (bez DPH)** | **Počet jednotek** | **Náklady na 5. rok provozu (bez DPH)** | **Celkové náklady na provoz bez DPH** | **Celkové TCO bez DPH** | **Celkové TCO vč. 21% DPH** |
| **Rozpočet - plnění části A - Dodávka licencí nástroje a instalace** | | | | | 700 000,00 Kč |  |  | | | | | | | | | | | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| Licence nástroje IdM | ks | VYMAZÁNO | VYMAZÁNO | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| *Další výše neuvedené (přidejte řádky)* | ks | VYMAZÁNO | VYMAZÁNO | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| **Rozpočet - plnění části B - Služby dle specifikace v Příloze 1 Smlouvy** | | | | | 820 000,00 Kč |  | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| Provedení vstupní analýzy | člověkohodina | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| Implementace IdM | člověkohodina | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| Zpracování související dokumentace | člověkohodina | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| Provedení migrace na nový HW | člověkohodina | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| Poskytování služeb rozvoje | člověkohodina | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| *Další výše neuvedené (přidejte řádky)* | člověkohodina | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| **Rozpočet - plnění části D - Provozní podpora - Zadavatel stanoví maximální cenu na 1 500 000,- Kč bez DPH za plnění dle této části rozpočtu (buňka R18)** | | | | | | | | | | | | | | | |  | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| **Provozní podpora Díla** | | | | | | | | | | | | | | | |  |  |  | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| Poskytování provozní podpory systému | měsíc | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) | [VYMAZÁNO](mailto:jan.budar@nudz.cz) |
| **CELKOVÉ NÁKLADY (TCO)** |  |  |  |  | **1 520 000,00 Kč** |  |  | **200 400,00 Kč** |  | **200 400,00 Kč** |  | **200 400,00 Kč** |  | **200 400,00 Kč** |  | **200 400,00 Kč** | **1 002 000,00 Kč** | **2 522 000,00 Kč** | **3 051 620,00 Kč** |

35

63

**SPECIFIKACE ŘEŠENÍ**

**NUDZ - Dodávka systému Identity managementu II.**

### Specifikace návrhu SW architektury

Kapitola obsahuje popis navrhovaného řešení systému Identity managementu od společnosti C SYSTEM CZ a.s. (dále také „cIDM“) s přihlédnutím k požadavkům zadavatele, jak jsou vyjádřeny v zadávací dokumentaci.

Identity management je chápán jako univerzální systém pro správu identit uživatelských oprávnění v heterogenním informačním systému v rámci podnikové sítě. Výkonné jádrové struktury zachycují stav „zde a nyní“, obsahují vše, co je třeba pro standardní běžnou službu, tedy zejména poskytování seznamů identit a seznamů oprávnění či rolí, dané identity v daném kontextu či v dané doméně. Doménou může být informační systém, budova nebo areál. V rámci domény jsou definovány role pro omezení řízení přístupu.

Systém disponuje možností napojení na zdrojové systémy pro čerpání informací o identitách. Dle dostupných informací může řídit životní cyklus identity od jejího vstoupení v platnost až do ukončení platnosti. V průběhu životního cyklu má uživatel možnost pomocí portálu spravovat svoje základní údaje, které nejsou čerpány ze zdrojových systémů, nahlížet na svoje oprávnění a zvolit na omezenou dobu svého zástupce, nebo delegovat svoje přístupy na jinou identitu.

Systém disponuje grafickým rozhraním pro správce, které umožní nastavení oprávnění pro jednotlivé identity, také automatické přiřazení oprávnění dle definovaných parametrů dostupných v organizační struktuře a zdrojovém systému. Akce prováděné uživateli v systému podléhají logování. Pomocí grafického rozhraní je možné vytvářet reporty pro kontrolu nastavení systému a oprávnění v něm

Systém poskytuje informace o identitách a jejich oprávněních pomocí rozhraní webových služeb SOAP a REST s podporou SSO, OAuth 2 a SAML standardů. Systém umožní napojeným systémům do cIDM vložit rozsah svých podporovaných rolí pro kontrolu integrity. V případě změny v oprávnění uživatele umožní odeslání notifikace napojeným systémům, které si notifikaci „předplatili“.

### Popis architektury řešení Identity managementu Popis použitých technologií, včetně popisu spuštění systému

Dodávané řešení cIDM není závislé na konkrétním hardware, virtualizační platformě či operačním systému. Navrhované řešení využije těch prvků, které jsou k dispozici, jak jsou popsány v zadávací dokumentaci.

Navrhujeme tedy virtualizační platformu VMware vSphere 6.x operační systém Microsoft Windows min verze 2012 R2 Server Standard, MS IIS 8.5 ).

Uživatelské prostředí cIDM je budováno pomocí open-source frameworku pro vývoj webových aplikací Angular 11.2.1. Uživatelské rozhraní je ralizováno jako single-page webová aplikace, která běží na koncovém zařízení ve všech standardních webových prohlížečích.

Výkonné jádro cIDM je vybudováno v datové platformě IRIS společnosti InterSystems. Při nasazení předpokládáme verzi InterSystems IRIS for Health 2020.x . InterSystems zajišťuje technickou podporu a aktualizační program pro IRIS, vždy ve spolupráci s dodavatelem aplikace.

Datová platforma IRIS bude pro cIDM standardním způsobem realizovat:

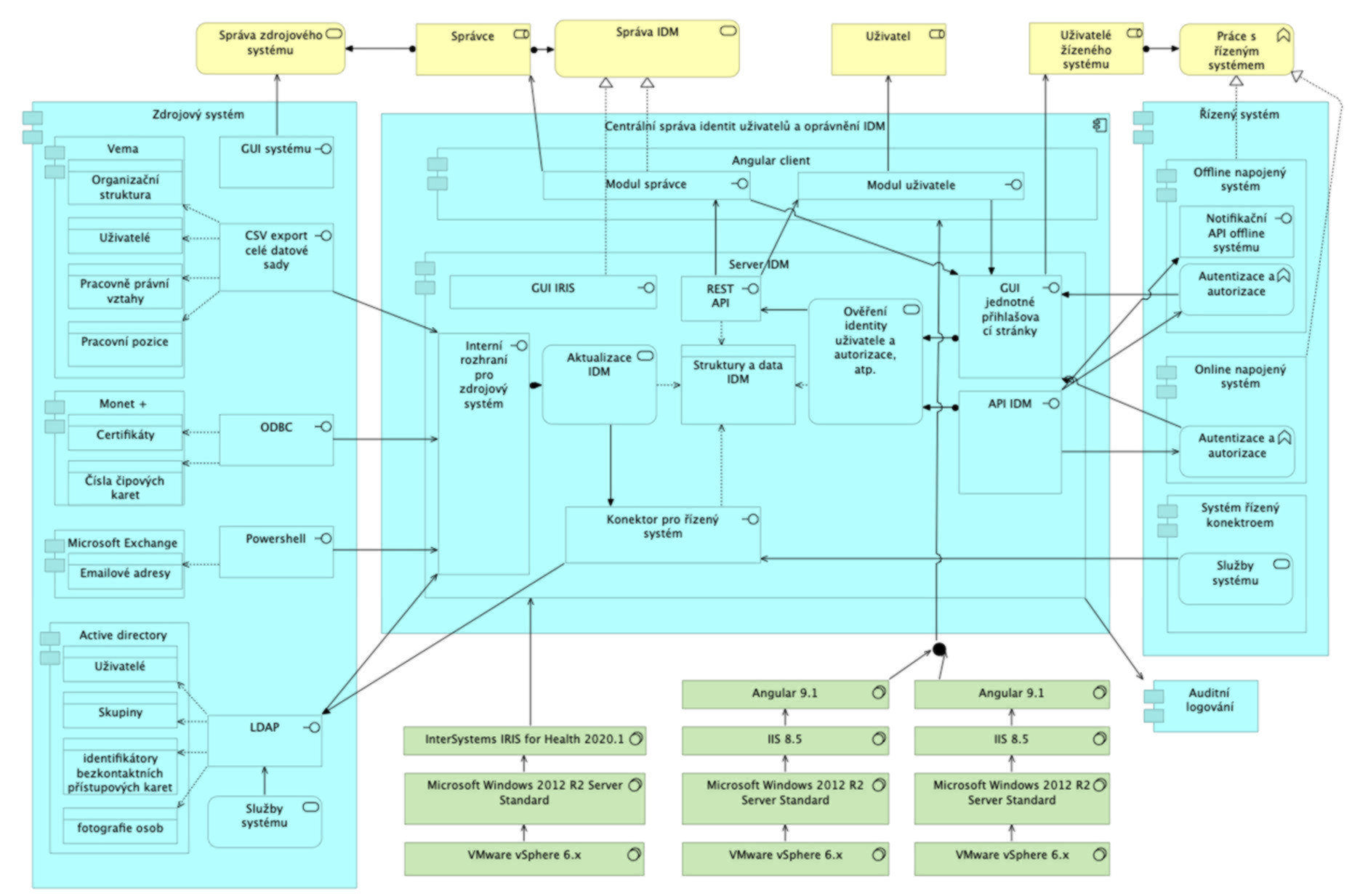
* databázové prostředí pro všechny typy dat (provozní, konfigurační, dočasná, strukturální, atd.)
* běhové prostředí pro skriptovací jazyk pro veškerou databázovou a aplikační logiku
* prostředí pro vývoj objektově orientovaných komponent cIDM, jejich metod a persistentních i transientních vlastností
* prostředí pro vývoj, konfiguraci a provoz všech interoperabilních komponent. (viz

*kapitola b Popis integračního rozhraní systému*.)

* IRIS obsahuje rozsáhlý správcovský portál, jehož prostřednictvím bude možné vykonávat nestandardní složité práce, týkající se analýz, auditů, konfigurací a řešení nestandardních situací

Vlastní vývoj dodavatele se týká všech částí a komponent cIDM, s využitím možností a stavebních bloků obsažených ve vývojových a provozních platformách uvedených výše (IRIS, Angular), zejména:

* datových struktur; databázové a aplikační logiky
* komunikačních a integračních komponent; konfigurace adaptérů, tvorba business procesů, služeb a operací, realizujících napojení systému na vnější prostředí
* grafického uživatelského rozhraní. Responzivní web design aplikace zajišťuje optimalizaci grafického uživatelského rozhraní pro různé druhy zařízení (tablet, mobilní telefon, notebook nebo PC) a jeho univerzální použitelnost ve všech standardních prohlížečích.



*Obr.1 Aplikační architektura řešení*

### Technická specifikace vrstev systému

**Virtualizační platforma** dostupná v prostředí zákazníka VMware vSphere 6.x s dokumentací dostupnou zde: https://docs.vmware.com/en/VMware-vSphere/index.html

**Operační systém** Microsoft Windows 2012 R2 Server Standard, MS IIS 8.5) s dokumentací dostupnou zde: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows- server-2012-r2-and-2012/hh801901(v=ws.11)

**Uživatelské prostředí** cIDM je budováno pomocí open-source frameworku pro vývoj webových aplikací Angular 9.1. s dokumentací dostupnou zde: https://v9.angular.io/docs

**Výkonné jádro cIDM** je vybudováno v datové platformě IRIS společnosti InterSystems. Při nasazení předpokládáme verzi (InterSystems IRIS for Health 2020.x) https://docs.intersystems.com/irisforhealthlatest/csp/docbook/DocBook.UI.Page.cls

Aplikační komponenty, které jsou součástí navrhovaného řešení systému cIDM, jsou popsány dále v tomto dokumentu.

### Zabezpečení dat

proti zneužití a poškození se opírá o možnosti poskytované datovou platformou IRIS. Vlastní vývoj cIDM těchto možností využívá, jak uvedeno dále a v žádném případě toto zabezpečení nekompromituje.

### Zabezpečení komunikace

Veškerá komunikace platformy s ostatními systémy je zabezpečená prostřednictvím TLS 1.2. Ověřování certifikátů klientských systémů není obecně vyžadováno mimo komunikační kanály, pro které není možná jiná forma autentizace.

Při komunikaci jednotlivých komponent řešení, které jsou nasazené uvnitř zabezpečené sítě a klienta při komunikaci je možné autentizovat jinak než prostřednictvím TLS, není šifrování nutně použito.

### Autentizace a autorizace

cIDM zabezpečuje služby autentizace a autorizace, detaily jsou uvedeny dále v nabídce. Těm komponentám, které podporují protokoly IHE, nabízí cIDM služby v souladu s profilem IUA a XUA.

Dle všeobecně doporučovaných postupů umožňuje přihlášení prostřednictvím jednotné přihlašovací stránky a poskytuje napojeným doménám autentizační/autorizační token v souladu s IUA, kdy řešení vystupuje v rolích aktérů Authorization Client a Resource Server podle IUA a autentizace/autorizace probíhá pomocí Authorization Code Grant Flow podle OAuth2. Autentizace/autorizace pro administraci systému pomocí Terminálu je zajištěna prostřednictvím Password Grant podle OAuth2. Také jako X-Service User a X-Service Provider podle profilu XUA (Cross-Enterprise User Assertion). Ne všechny služby tuto úroveň zabezpečení vyžadují/podporují. V takových případech se jedná o komunikaci, která je zabezpečena použitím TLS v1.2 spolu s autentizací pomocí certifikátů, případně ověřením jména a hesla systémového účtu klienta.

### Zabezpečení dostupnosti

Zabezpečení dostupnosti se opírá o možnosti poskytované datovou platformou IRIS. Pro zajištění dostupnosti jsou v rámci navrhovaného řešení pro produkční prostředí navrženy 2 webové servery, které umožní load balancing požadavků přicházejících na server.

### Zabezpečení důvěrnosti informací

Data jsou chráněna datovou platformou IRIS a zabezpečením komunikačních kanálů, jak je naznačeno výše. Dále je vhodné, aby zadavatel zajistil ochranu databázových a žurnálových souborů platformy, pokud chce zajistit ve svém vnitřním prostředí snížené riziko kompromitování dat v cIDM. Žurnálování dat je sice možné omezit, v provozním systému by se tím nepřijatelně snížila bezpečnost a dostupnost systému.

* OS – přístup k databázovým souborům by měl být zabezpečen omezením přístupu uživatelů OS k tomuto souboru. Čtení může být povoleno pouze pro systémového uživatele, pod kterým běží procesy IRIS s aplikačním kódem řešení, případně také hlavnímu administrátorovi systému.
* Diskové pole/virtualizace – Kompromitace souborů virtuálních disků virtuálních strojů, na kterých bude nasazeno cIDM, představuje nízké riziko z hlediska čtení dat z databázových souborů existujících v rámci těchto virtuálních disků. Toto riziko je nicméně možné ještě více snížit pomocí šifrování souborů virtuálních disků na úrovni virtualizační vrstvy nebo diskového pole.

### Auditní logování

Systém cIDM lze konfigurovat pro zaznamenávání různých typů událostí do zabezpečeného auditního logu. Pokud uživatel disponuje centrálním auditovacím systémem, (například dle IHE profilu ATNA), cIDM jej umí využít a posílat auditovací záznamy do centrálního systému standardizovaným způsobem.

### Reporting

V rámci systému lze v čase získávat reporty o stavu systému a jeho nastavení pomocí informačních textů na vyžádání. Pro tyto informační texty lze také nadefinovat jejich odesílání v návaznosti na změny v organizační struktuře a oprávněních.

Mimo výše zmíněnou funkcionalitu disponuje platforma IRIS řadou vestavěných reportů monitorujících stav systému a dostupných prostředků, které se dají spouštět manuálně, nebo dle definovaného časového plánu. Obsah reportu je možné vytvářet na míru různých potřeb organizace.

### Zprávy pro včasné varování a zásah

Systém disponuje konfigurovatelnou funkcionalitou informačních textů. V návaznosti na události v rámci životního cyklu entity a organizační struktury je entitě vygenerován informační text, který jí seznámí s rozsahem oprávnění v jednotlivých informačních systémech, která jsou v rámci cIDM definována. Tento text je následně entitě odeslán do její e-mailové schránky. Stejně tak v případě změny v oprávněních, nebo změně vztahu k organizační struktuře je entita informována o jejich změně.

Vlastní provádění notifikace je konfigurovatelné pro příjemce, původce notifikace, správce systému, který je změnou v oprávněních ovlivněn

Pro komunikaci mezi systémy je v rámci cIDM k dispozici mechanismus notifikace řízeného systému, kdy v návaznosti na změny v oprávněních a změny v rámci životního cyklu entit je možné napojeným systémům předávat informace o změnách zasláním identifikátorů uživatelů se změnou. V návaznosti na tuto notifikaci může napojený systém využít odpovídající služby pro synchronizaci oprávnění uživatele.

Notifikace může napojený systém přijímat pomocí webové služby (REST, SOAP), nebo pomocí souboru.

Notifikace o změnách může probíhat také zasláním celého seznamu oprávněných uživatelů a jejich oprávnění pro daný systém ve formátu CSV, XML

### Popis integračního rozhraní systému

Systém cIDM se připojuje a komunikuje ve dvou záležitostech:

1. cIDM vystupuje jako správce přístupů (Access Manager) a
2. cIDM získává zdrojová a konfigurační data ze zdrojových systémů. Daný systém může komunikovat v obou záležitostech, tedy zároveň poskytovat data (například o uživatelích) a zároveň být řízen z pohledu uživatelských práv.

### Access Manager (také Přístupová struktura)

### Obecný popis napojení řízeného systému

Komunikace s řízenými systémy probíhá pomocí standardního rozhraní, pomocí kterého systémy konzumují změny v oprávněních a pracovních vztazích, nebo aktualizují celou databázi entit, jejich oprávnění, nebo organizační struktury.

Pro řízené systémy je zřízen konektor, který využívá API daného sytému a umožní jeho řízení přímo z cIDM.

Řízené systému mohou pro nastavení k nim importovat do cIDM jejich strukturu rolí pomocí CSV, nebo XML.

### Autentizační mechanismy

Systém disponuje vestavěnými autentizačními mechanismy pro ověření pomocí jména a hesla. Dále umožňuje dalších autentizačních mechanismů v rámci organizace jako jsou autentizace tokenem, pomocí biometrických údajů.

### Podporované standardy

### OAuth 2.0

OAuth 2.0 (RFC 6749) je moderní autorizační protokol (resp. framework) pro bezpečnou API autorizaci jednoduchým a jednotným způsobem pro webové i desktopové aplikace. Jeho specifikace popisuje podrobně fungování oné výše popsané výměny tokenů a klíčů; nijak nedefinuje vlastní komunikaci s webovou aplikací ani není vázané na konkrétní typ API (pouze je omezeno na HTTP protokol). OAuth lze tedy použít jako metodu ověření uživatele k jakémukoli typu API (SOAP, XML-RPC, REST atd.), a to nejen na webových aplikacích.

### OpenID Connect

Protokol OpenID Connect je nadstavba nad OAuth 2.0 která umožňuje provádět autentizaci uživatelů pro napojené systémy. Podrobnou dokumentaci lze nalézt zde: (https://openid.net/specs/openid-connect-core-1\_0.html)

### IUA/JWT

IHE profil Internet User Authorization (IUA) definuje konkrétní vlastnosti komunikace a předávaných bezpečnostních tokenů pomocí frameworku OAuth 2.0 pro použití ve zdravotnickém prostředí. Tato rozšíření jsou plně kompatibilní i s protokolem

OpenID Connect a lze je tedy vzájemně kombinovat. Specifikace tohoto profilu je dostupná on-line na níže uvedeném odkazu: https://[www.ihe.net/uploadedFiles/Documents/ITI/IHE\_ITI\_Suppl\_IUA.pdf](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_IUA.pdf)

cIDM podporuje fungování v roli aktéra Authorization Server podle profilu IUA včetně možnosti SAML Token Option.

### XUA/SAML

Jako součást autorizačních tokenů bude cIDM klientským systémům předávat i

SAML Assertion. Získanou SAML Assertion nesoucí autentizační i autorizační položky pro uživatele mohou klientské systémy následně použít pro autentizaci/autorizaci IHE transakcí

podle profilu XUA (https://[www.ihe.net/uploadedFiles/Documents/ITI/IHE\_ITI\_TF\_Vol2b.pdf#nameddest=3\_4](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf#nameddest%3D3_4)

0\_Provide\_X\_User\_Assertion )

### Zdrojové systémy

### Obecný princip napojení na zdrojové systémy

Jako zdrojový systém je chápán systém udržující informace o různých entitách v rámci organizace. Těmi mohou být zaměstnanci, dodavatelé, zákazníci, auditoři, systémy hardware a další. Zdrojové systémy můžou dále poskytovat informace o organizační struktuře a vztazích jednotlivých entit k organizační struktuře.

Napojení na zdrojový systém probíhá formou neinvazivní, tudíž provoz zdrojového systému by neměl být narušen napojením cIDM a zátěž na zdrojový systém by měla být co nejmenší. Vlastní napojení je realizováno jak přírůstkovou synchronizací tak exportem celé databáze uživatelů. Může být realizováno pomocí standartního rozhraní např. LDAP nebo cestou importu souborů ve formátu CSV, XML, JSON resp. využitím voláním webové služby. Dalším ze způsobů napojení je přímé načítání dat z databáze realizované pomocí ODBC driverů nebo podobných řešení.

Mezi základní zdrojové systémy patří:

* + Personální systém
  + CRM systém
  + Active Directory
  + PKI systém

### Konektory systému

### Automatické propisování do napojených systému

Komunikace s napojenými systémy probíhá pomocí standardního rozhraní. Jako alternativní způsob napojení systémů lze vytvořit konektor pro jednotlivé systémy, pomocí kterých budou systémy konzumovat změny v oprávněních nebo aktualizovat celou databázi uživatelů a jejich oprávnění.

Konektor může být realizovaný jako:

* napojení na API systému, přes které je možné v systému zakládat uživatele a jejich oprávnění
* vytvoření exportu pro daný systém, který si následně zpracuje.

Systém disponuje možností vytvořit libovolný konektor.

### Manuální propisování do napojených systému

Konektory pro systémy, které nejsou schopny konzumovat standardní rozhraní, přijímat informace o entitách pomocí vystavení webové služby ani zpracování exportu, musí být realizovány operátorem/správcem daného systému. Jejich vlastní realizace záleží na dostupných možnostech systému.

### Konektor na Active Directory

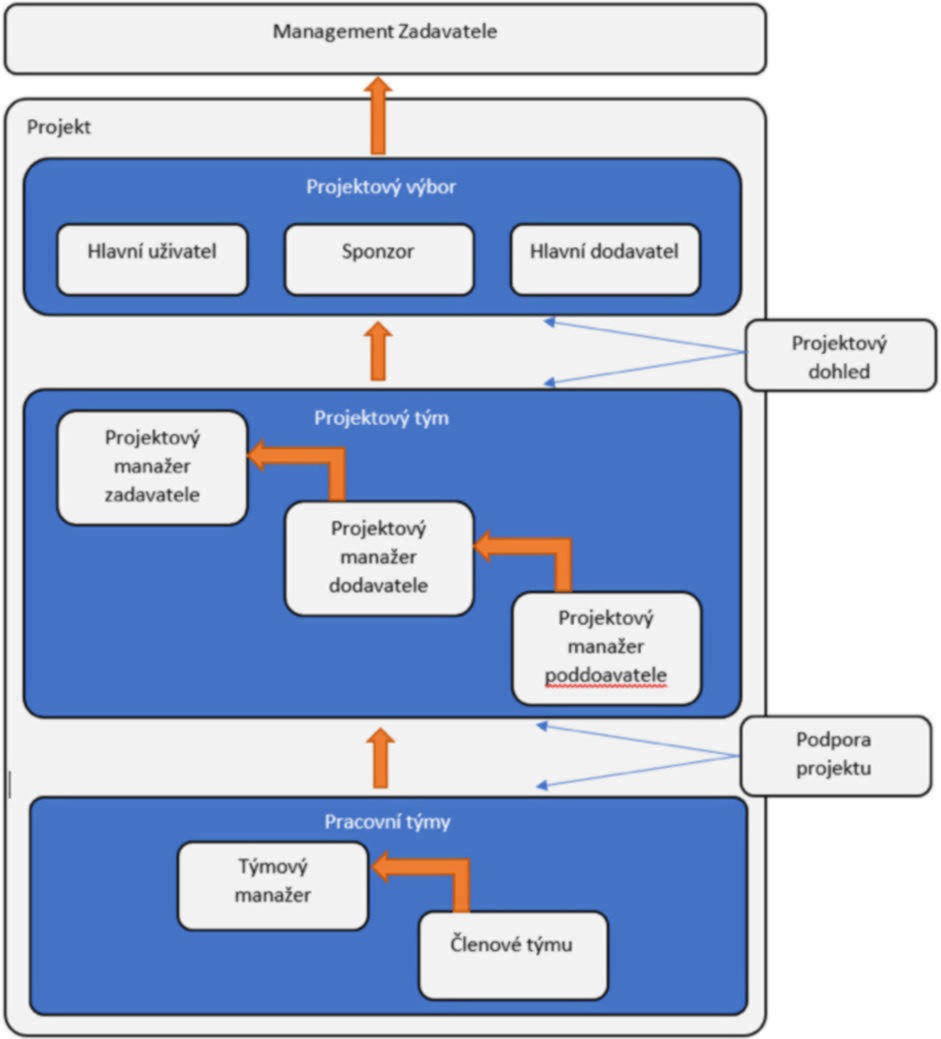
Pro Active Directory disponuje cIDM konektorem umožňujícím základní práci s daty uživatelů jako jsou úpravy informací o uživateli, změna a obnova hesla. Díky tomuto konektoru je umožněna správa skupin v Active Directory a správa vazeb mezi uživatelem a skupinou.

V rámci tohoto konektoru umožňuje cIDM správu přístupu ke sdíleným síťovým prostředkům v rámci systému Windows pro jednotlivé uživatele.

### Organizačně technické zajištění plnění předmětu veřejné zakázky

### Postup implementace cIDM

### Organizace, role a odpovědnosti



*Obr.2 Schéma rolí v organizaci projektu*

V rámci řízení projektů rozdělujeme organizaci projektu do třech skupin:

### Skupina Rozhodování – Projektový výbor.

Projektový výbor poskytuje celkové směřování projektu, zajišťuje zdroje (lidské zdroje, vybavení a pod)., provádí hlavní rozhodování a schvalování plánů a výstupů projektu (akceptace). Členy projektového výboru jsou:

### Supervisor (sponzor) projektu

Supervizor zastupuje zájmy Zadavatele, má hlavní rozhodovací pravomoc na projektu, zajišťuje financování projektu a má celkovou odpovědnost za úspěch projektu. Schvaluje a odvolává vedoucího projektu (Projektového manažera) Zadavatele, má právo svolat Projektový výbor. Obvykle je Sponzorem projektu člen vrcholového managementu Zadavatele. Jedná se o jednu osobu s nedelegovatelnou odpovědností za úspěch projektu, vede projektový výbor a má v něm rozhodující slovo.

### Hlavní uživatel projektu

Reprezentuje zájmy uživatelů, poskytuje uživatelské zdroje, podporuje a udržuje pozornost na požadovaný výsledek projektu. Specifikuje požadavky a zajišťuje přijetí ze strany uživatelů.

Zajišťuje, že produkty projektu jsou používány, a tudíž mohou být dosaženy, přínosy projektu. Definuje očekávání zákazníka na kvalitu a akceptační kritéria.

### Hlavní dodavatel projektu

Člen Projektového výboru zastupující zájmy dodavatele. Poskytuje dodavatelské zdroje nezbytné pro dodávání produktů. Informuje o odborných aspektech projektu, jako je např. technická proveditelnost. Odpovídá za kvalitu produktů.

### Projektový dohled

Projektový dohled zajišťuje zainteresovaným stranám projektu, že projekt postupuje správně. Toto je odpovědnost výše uvedených členů Projektového výboru, ale lze ji delegovat např. i na interní nebo externí osoby (z pohledu Zadavatele). Projektový dohled musí být nezávislý vůči projektovému manažerovi, projektové podpoře a Týmovým manažerům.

### Skupina Řízení – Projektový tým.

Projektový tým je řízen projektovým manažerem Zadavatele a členy jsou projektoví manažeři dodavatele a poddodavatelů.

### Projektový manažer Zadavatele

Projektový manažer zodpovídá za denní řízení projektu, je oprávněn svolávat Projektový výbor, na kterém reportuje o stavu projektu. Jedná se o jedinou osobu, která zodpovídá za plnění klíčových milníků projektu, navrhuje projektový plán, navrhuje definici projektu. V rámci plnění projektu má kompetenci vymáhat plnění úkolů napříč celou organizací. Odchylky, výjimky a nová rizika projektu předkládá ke schválení Řídícímu výboru, při operativním jednání supervisoru projektu. Definuje a řídí Pracovní týmy Zadavatele.

### Projektový manažer dodavatele

Projektový manažer dodavatele je podřízený projektovému manažeru Zadavatele. Zodpovídá za vytváření plánů dodávky produktů a monitoruje stav produktů. Reportuje Projektovému manažerovi Zadavatele a účastní se Projektových výborů, kde reportuje stav projektu za stranu dodavatele. Má právo svolat mimořádný Projektový výbor. Svoji činnost reportuje Hlavnímu dodavateli projektu. Je jmenován a odvoláván Hlavním dodavatelem projektu.

### Projektová podpora

Poskytuje administrativní podporu projektu, poradenství, projektové návody a metodickou pomoc. Jedná se o odpovědnost projektových manažerů, ale může být delegována.

### Skupiny Poskytování – Pracovní týmy

Úkolem pracovních týmů je realizovat dílčí projektové úkoly a dodávat tak produkty projektu s potřebnými výstupy. Pracovní týmy jsou stanovovány pro konkrétní části projektů a jsou definovány buď projektovým manažerem dodavatele (pokud se týká práce čistě na straně dodavatele) anebo projektovým manažerem Zadavatele (pokud se jedná o dodání potřebné součinnosti anebo o společný tým Zadavatele a Dodavatele). V čele pracovního týmu je vždy určen Týmový manažer. Definice jednotlivých projektových týmů bude provedena v rámci Prováděcího projektu.

### Týmový manažer

Týmoví manažeři jsou zodpovědí za dodání produktů / vytvoření výstupů projektu. Řídí členy pracovního týmu, reportují Projektovému manažerovi.

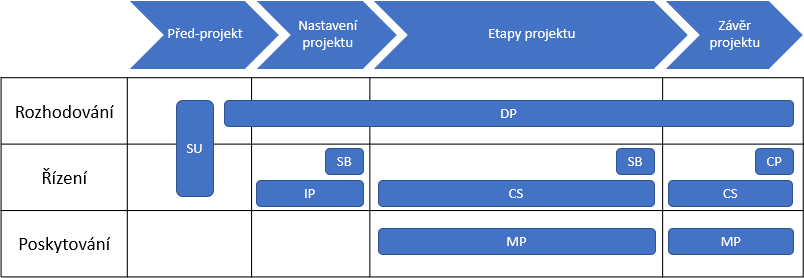
### Členové týmu

Pro jednotlivé implementační, konzultační a podpůrné činnosti jsou určeni konkrétní členové pracovních týmů. Jejich výběr, koordinaci a řízení jejich práce má na starosti týmový manažer.

### Procedury a standardy řízení implementace

Celý projekt „Dodávka systému Identity Managementu II“ bude řízen dle metodiky PRINCE 2 týmem zkušených projektových manažerů, kteří jsou zárukou zvládnutí celého procesu implementace a dosažení požadovaných výstupů – přínosů projektu.

V této části nabídky uvádíme základní principy vedení implementace, detailní zpracování jednotlivých bodů bude uvedeno v dokumentu *Nastavení projektu*, který bude předložen do 5 pracovních dní od nabytí účinnosti smlouvy o dílo v rámci Prováděcího projektu.



*Obr.3 Schéma řízení implementace*

|  |  |  |
| --- | --- | --- |
| **Proces** | **Proces (EN)** | **Zkratka** |
| Zahájení projektu | Starting up a Project | SU |
| Směřování projektu | Directing a Project | DP |
| Nastavení projektu | Initiating a Project | IP |
| Kontrola etapy | Controlling a Stage | CS |

|  |  |  |
| --- | --- | --- |
| Řízení dodávky produktu | Managing Product Delivery | MP |
| Řízení přechodu mezi etapami | Managing a Stage Boundary | SB |
| Ukončení projektu | Closing a Project | CP |

### SU – Zahájení projektu

Tento proces musí proběhnout na straně zadavatele – pravděpodobně již proběhl – a jeho cílem je zvážit, zda je projekt realistický a zda má smysl jej iniciovat. Vychází se přitom z hrubých odhadů na náklady, čas, organizační strukturu a podobně. Zároveň tento proces stanovuje požadované přínosy a výstupy celého projektu, definice očekávané kvality, definice akceptačních kritérií. V rámci Zahájení projektu je určen tzv. Sponzor projektu.

### DP – Směřování projektu

Směřování projektu je průběžný proces probíhající v rámci celého projektu. Směřování je prováděno tzv. Projektovým výborem, který provádí přezkoumání informací, poskytuje klíčová rozhodnutí a zajišťuje komunikaci s managementem zadavatele. Směřování projektu také říká, jak by rada projektu měla autorizovat plán etapy, včetně plánů na zpracování výjimky – pokud by nastala. Tento proces také pokrývá ad-hoc řízení a jak by měl být projekt uzavřen. Mezi klíčové aktivity patří: autorizace nastavení projektu, autorizace plánu etapy nebo výjimky, ad- hoc řízení a potvrzení uzavření projektu.

### IP – Nastavení projektu

Tento proces nastavuje pevné základy celému projektu. Vzniká dokumentace Nastavení projektu, což je základní řídící dokument projektu. Tento dokument obsahuje:

Upřesnění zadání dle Charty projektu

* Strategie řízení rizik
* Strategie řízení změn
* Strategie řízení kvality
* Strategie řízení komunikace
* High-level plán projektu
* Definice projektových kontrol

Nastavení projektu je následně předáno Projektovému výboru ke schválení.

### CS – Kontrola etapy

Cílem tohoto procesu je autorizace a předávání balíků práce. V procesu je specifikováno, jak by měl být monitorován postup a jak informovat Projektový výbor o postupu. V tomto procesu jsou také metody, jak by měly být eskalovány některé výjimky v projektu. Klíčové aktivity procesu jsou: schválení pracovních balíků, vyhodnocení postupu, zachycení a zhodnocení výjimek v projektu, monitorování a kontrola rizika, posouzení stavu etapy, hlášení významných událostí, provedení nápravných akcí, eskalování projektových výjimek a přijímání hotových pracovních balíků.

### MP – Řízení dodávky produktu

Řízení dodávky produktu zajišťuje propojení mezi projektovým týmem a týmovými manažery pomocí formálních požadavků na akceptování, provádění a dodávaní projektové práce. Hlavními cíli tohoto procesu jsou:

* + zajištění, aby práce týmů na produktech byla schválena,
  + týmový manažeři, členové týmů a dodavatelé měli jasnou představu, co má být dodáno z hlediska očekávaného úsilí, nákladu, času a kvality,
  + plánované produkty jsou doručeny s požadovanými vlastnostmi a v rámci tolerance,
  + projektovému manažerovi je v pravidelných a dohodnutých intervalech podávána zpráva, o postupu prací

Klíčové aktivity tohoto procesu jsou odsouhlasení balíku práce a vykonání a dodání balíku práce.

### SB – Řízení přechodu mezi etapami

Řízení přechodu mezí etapami říká, co by mělo hotové na konci etapy. Především by měla být naplánována další etapa a měla by být provedena aktualizace celého projektového plánu. V tomto procesu se také aktualizuje obchodní případ a registr rizik. Proces také pokrývá, co by se mělo udělat, pokud etapa přesáhne dané tolerance. Nakonec tento proces specifikuje, jak by měl být reportován konec etapy.

Klíčové aktivity procesu jsou plánování následující etapy, aktualizace projektového plánu, aktualizace obchodního případu, aktualizace registru rizik, zpráva o konci etapy a vytvoření plánu výjimky.

### CP – Ukončení projektu

Tento proces obsahuje činnosti, které by se měly provést na konci projektu. Projekt by měl být formálně ukončen (a zdroje uvolněny pro jiné aktivity), následující akce by měly být identifikovány a projekt sám o sobě by měl být formálně zhodnocen. Mezi klíčové aktivity tohoto procesu patří ukončení projektu, identifikování po-projektových činností, předání produktů, vyhodnocení projektu, vyhodnocení přínosů (už dosažených a aktualizovat předpovědi pro ostatní přínosy a naplánování vyhodnocení těch přínosů, které ještě nebyly dosažené).

### Harmonogram prací

|  |  |  |
| --- | --- | --- |
| **Harmonogram projektu - fáze a etapy** | **Termín zahájení** | **Termín ukončení** |
| **Část plnění** |  | |
| **Etapa I. - Příprava a pořízení IS** | | |
| 1.1 Zajištění projektu - komplexní a detailní  řízení projektu a jeho realizace | Po účinnosti Smlouvy | Do doby Kompletní akceptace díla |
| 1.2 Provedení vstupní analýzy a schválení návrhu implementace | Po účinnosti Smlouvy | DO 30 DNÍ PO ÚČINNOSTI SMLOUVY |
| 1.3 Dodávka potřebných licencí cIDM | Do 30 dní po účinnosti Smlouvy | Do 30 dní po účinnosti Smlouvy |
| **Etapa II. – Nasazení systému** | | |
| 2.1 Implementace cIDM do architektury NUDZ | Do 30 dní po účinnosti Smlouvy | Do 90 dní po účinnosti Smlouvy |
| 2.2 Integrace systému do prostředí Zadavatele | Do 91 dní po účinnosti Smlouvy | Do 120 dní po účinnosti Smlouvy |
| 2.3 Zajištění pilotního provozu | Do 121 dní po účinnosti Smlouvy | Do 153 dní po účinnosti Smlouvy |
| 2.4 Migrace dat | Do 153 dní po účinnosti Smlouvy | Do 167 dní po účinnosti Smlouvy |
| 2.5 Zpracování související dokumentace | Do 153 dní po účinnosti Smlouvy | Do 167 dní po účinnosti Smlouvy |
| 2.6 Migrace na nový HW | Po závazném pokynu Objednatele | Do 15 dní po závazném pokynu Objednatele |
| **Etapa III. – Akceptace** | | |
| 3.1 Kompletní akceptace Díla (KAP) | Po závazném pokynu Objednatele | Do 6 měsíců od účinnosti smlouvy |
| **Etapa IV. - Provozní fáze (fáze udržitelnosti) projektu** | | |
| 4.1 Poskytnutí záruky na celé řešení | Převzetí Díla | 60 měsíců od převzetí Díla, minimálně do doby 31. 10. 2026 |
| 4.2 Poskytnutí provozní podpory informačního systému v rámci nezpůsobilých  nákladů projektu |
| 4.3 Poskytování služeb rozvoje (úprav Díla) |

V rámci jednotlivých výše uvedených etap budou realizovány následující služby:

### Etapa I

* Zahájení projektu, příprava dokumentu Nastavení projektu, odsouhlasení pravidel a strategie projektu, založení Projektového výboru.
* Analýza požadavků
  + Provedení technické analýzy systémů a evidencí napojených do cIDM.
  + Analýza požadavků na bezpečnost systémů a požadavků na jejich provoz.
  + Provedení analýzy organizačních aspektů souvisejících se správou a provozem systémů a analýza životního cyklu uživatelských identit a návrh způsobu jejich naplnění.
* Návrh, projednání a schválení implementace
* Stanovení požadavků na součinnost Poskytovatelů zapojených systémů
* Dodávka potřebných licencí pro DB a licencí pro produkt cIDM

### Etapa II

* Instalace cIDM na poskytnutý HW a zpřístupnění systému vybraným pracovníkům Objednatele, kteří se budou podílet na správě systému.
* Úpravy řešení dodaného systému tak, aby plně odpovídal požadavkům zadání.
* Nastavení životního cyklu uživatelských identit a přístupových oprávnění a napojení na systémy, které s identitami pracují (personální systém, AD apod.).
* Testování systému
  + Provedení funkčních testů;
  + Provedení bezpečnostních testů
  + Vyhodnocení testování a realizace opatření z testování vyplývajících.
* Školení administrátorů systému (3 osoby).
* Napojení systémů Objednatele
* Zpracování související dokumentace
  + Zpracování technické dokumentace systému
  + Zpracování provozní dokumentace
* Provedení migrace na nový HW

### Etapa III

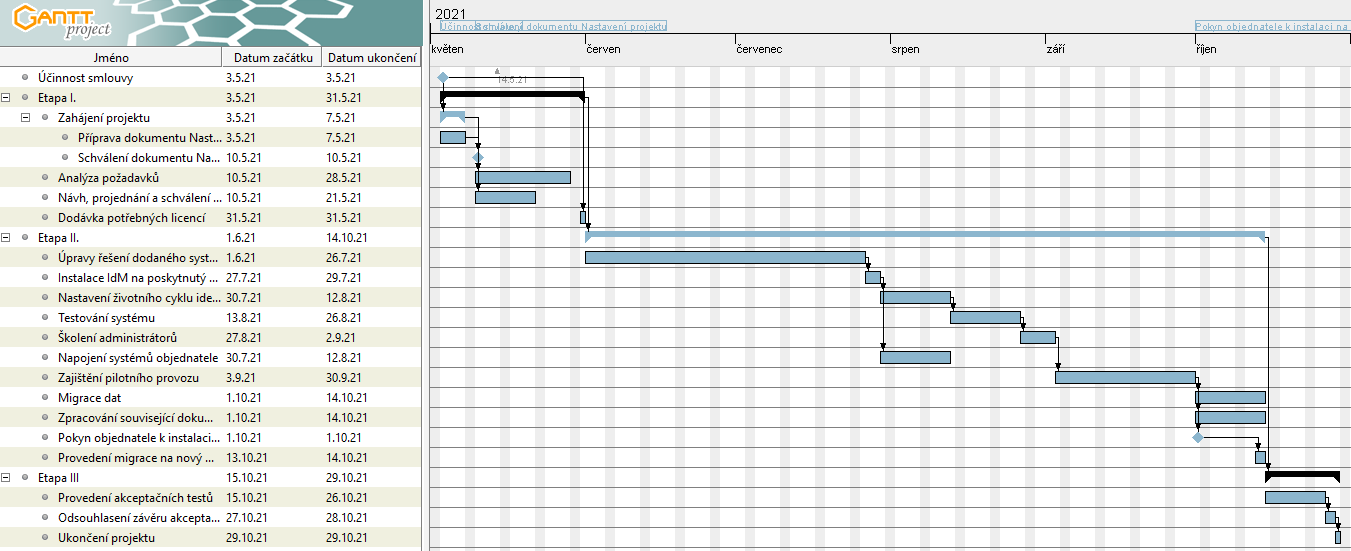
* Provedení akceptačních testů
* Odsouhlasení závěru akceptačních testů
* Ukončení projektu, finální akceptace

### Etapa IV

* Poskytnutí záruky na celé řešení
* Poskytnutí provozní podpory v rámci nezpůsobilých výdajů projektu
* Poskytnutí služeb rozvoje Systému



Příloha č. 4 Návrh poskytovatele



*Obr. 4 Časový harmonogram prací*

17

80

### Požadovaná součinnost ze strany zadavatele

|  |  |  |  |
| --- | --- | --- | --- |
| **Součinnost** | **Etapa** | **Odhad časové náročnosti / specifikace součinnosti** | **Potřebná odbornost** |
| Účast na procesu DP – Směřování projektu (v řídícím / projektovém výboru). Týká se Sponzora projektu, Manažera projektu za stranu Zadavatele, Hlavní uživatelé, Projektový dohled | Během celého projektu | Cca 1 x za 2 měsíčně na cca 1-2 hodiny | Sponzor – ideálně člen vrcholového managementu + Projektový manažer |
| Účast na procesu CS – Kontrola etapy v podobě kontrolních dnů projektových manažerů. Týká se Manažera projektu za stranu  Zadavatele a Hlavních / klíčových uživatelů | Během celého projektu | Cca 1 x 14 dní na  cca 2-3 hodiny | Projektový manažer  / šéf IT za hlavního uživatele |
| Účast na procesu SB – Řízení přechodu mezi etapami. Týká se Manažera projektu za stranu Zadavatele a Hlavních /  klíčových uživatelů | Při ukončení každé z etap projektu | Cca 1 pracovní den | Projektový manažer  + šéf IT za hlavního uživatele |
| Účast na procesu CP – Ukončení projektu. Týká se Manažera projektu za stranu Zadavatele a Hlavních / klíčových uživatelů | 1 x při ukončování projektu | Cca 1-2 pracovní dny | Projektový manažer  + šéf IT za hlavního uživatele |
| Konzultace s Hlavním a  s klíčovými uživateli, zpětné vazby, připomínky, dílčí akceptační procesy | Během celého projektu |  | Vybraní 2-3 uživatelé (za lékaře, sestry…) Uživatelé s chutí do IT, kteří mají přirozený respekt u kolegů a dostatečný nadhled  v jejich pracovní oblasti |
| Zajištění vzdáleného přístupu k HW infrastruktuře požité pro  předmětný projekt | Během celého projektu | Dle specifikace Zadavatele (např.  VPN…) |  |
| Zajištění komunikačního prostředí pro vzdálenou komunikaci / on-line jednání projektových a pracovních týmů Zadavatele a Uchazeče | Během celého projektu | Skype, Teams apod. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Nezbytná technická dokumentace popisující rozhraní napojovaných systémů | Etapa I |  |  |
| Příprava podkladů a poskytování zpětné vazby při tvorbě Analýzy prostředí a Návrhu implementace | Etapa I | Cca 3-5 pracovních dnů | Pracovníci  s výbornou znalostí prostředí, schopnosti získávat  / koordinovat získávání podkladů z nemocnice / technologické znalosti |
| Příprava / zajištění integrační části na straně stávajících systémů | Etapa II - Integrace systému do prostředí Zadavatele | Cca 3-5 pracovních dnů | Pracovníci, kteří mají na starosti stávající připojované systémy |
| Školení (účast školených uživatelů) | Etapa II - Zajištění pilotního  provozu |  | Vybraní koncoví uživatelé |
| Export a konsolidace dat pro migraci dat a popis exportovaných dat | Etapa II – Migrace dat |  | Určení administrátoři |
| Podpora při migraci na nový HW vč. detailního popisu nové  infrastruktury | Etapa II – Migrace na  nový HW | Cca 2-3 pracovních dní | Určení administrátoři |
| Účast administrátorů na převzetí systémů Integrační platformy | Etapa III – Akceptace | Cca 5-10 pracovních dní | Určení administrátoři |

Upřesnění výše uvedených požadavků na součinnost a jejich doplnění bude definováno jako součást vstupní analýzy.

### Popis naplnění uživatelských požadavků

### Základní požadavky

|  |  |  |
| --- | --- | --- |
| **Číslo požadavku** | **Popis požadavku** | **Způsob naplnění požadavku - popis funkce, standardní součást produktu nebo vývoj na klíč** |
| 1.1 | IdM umožňuje v adresářové službě a řízených informačních systémech Zadavatele synchronizaci lidí včetně jejich přístupových účtů a hesel tj. zejména zaměstnanců/dohod o provedení práce/pracovní činnosti, externistů, pacientů a subjektů výzkumu (nástup/ukončení zaměstnance/ externisty/pacienta/subjektu výzkumu, změna pracovní pozice/hospitalizace atd.). | Komunikace s řízenými systémy probíhá pomocí standardního rozhraní, pomocí kterého systémy konzumují změny v oprávněních a pracovních vztazích, nebo aktualizují celou databázi entit, jejich oprávnění, nebo organizační struktury.  Pro řízené systémy může být zřízen konektor, který využívá API daného sytému a umožní jeho řízení přímo z cIDM.  Pro Active Directory disponuje cIDM konektorem umožňujícím základní práci s uživatelem úpravy informací o uživateli, změnu hesla a jeho obnovu. Umožnuje správu skupin v Active Directory a správu vazeb mezi uživatelem a skupinou.  Řízené systému mohou pro nastavení k nim importovat do cIDM jejich strukturu rolí pomocí CSV, nebo XML. |

|  |  |  |
| --- | --- | --- |
| 1.2 | IdM umožňuje v adresářové službě a řízených informačních systémech Zadavatele synchronizaci organizačních útvarů a skupin (dominantní část činnosti Zadavatele se odehrává formou realizace projektů/grantů, použitý systém uživatelských práv/rolí tedy musí bezpodmínečně respektovat několik rovin práv/rolí:   1. v **organizační rovině** v souladu zejména s organizačním řádem Zadavatele (organizační útvary, zařazení zaměstnanců do nich, vztahy nadřízenosti a podřízenosti), 2. v **rovině finančních zdrojů** v souladu s vnitřním kontrolním systémem Zadavatele (typicky příkazce operace, správce rozpočtu, apod.), 3. v **rovině odpovědné osoby** (např. za místnost v případě evidence majetku, osoby, která majetek převzala apod.),   v **rovině ustanovené komise** (např. personální nebo likvidační) tj. specifických skupin s trvale jmenovanými členy, | Díky architektuře organizační struktury systému je možné v rámci organizační struktury zachytit veškeré požadované vztahy v organizaci. Organizační struktura umožnuje definici vztahů nadřízenosti a podřízenosti jednotlivých prvků, jejich příslušnosti k jinému uzlu a zachycení pracovně právních vztahů. Počet dimenzí organizační struktury není technologicky omezen.  V praxi bývá prvkem provisioning systému víceúrovňová multidimenzionální organizační struktura, která je schopna obsáhnout zároveň pracovně-právní organizační strukturu a projektovou organizační strukturu sjednocenou do jedné maticové struktury. Mimo základní popsané výše lze jmenovat zdroje financování, které k sobě mohou evidovat vztahy odpovědnosti a možnosti žádat jejich čerpání. V rámci organizační struktury lze definovat skupiny uživatelů plnící různé agendy v rámci organizace například finanční komise a další. |
| 1.3 | IdM umožňuje v adresářové službě a řízených informačních systémech Zadavatele synchronizaci servisních účtů (pro vnitřní potřebu IT systémů) a externistů (např. dodavatelé provádějící dočasné či průběžné servisní práce, dočasné stáže). | Zdrojem entit pro cIDM může být jeden nebo více externích systémů, který organizace využívá pro stávající správu. Typicky pro správu uživatelů připadá v úvahu napojení personálního systému, nebo CRM systému. Systém také uchovává účty, které nejsou  evidované ve výše zmíněných systémech, potřebné |

|  |  |  |
| --- | --- | --- |
|  |  | pro provoz infrastruktury a její správu. Tyto entity lze  spravovat přímo v cIDM. |
| 1.4 | IdM umožňuje v adresářové službě a řízených informačních systémech Zadavatele synchronizaci přístupových karet a fyzických přístupových úrovní v systému elektronické kontroly vstupu (ACS). | V rámci uchování informací o jednotlivých identitách se evidují různé rozšiřující informace včetně informací uložených na elektronických resp.  přístupových kartách. |
| 1.5 | Systém umožňuje tvorbu, synchronizaci, řízení, blokování a mazání identit, rolí a dalších potřebných objektů v centrální adresářové službě a informačních systémech řízených nástrojem IdM. | Nativní funkcí systému je obecná správa všech prvků v systému (entity, organizační struktura a vztahy) v rozsahu jeho založení, úpravy, blokování, čtení a definice jeho životního cyklu.  Pro zachování kompletní historie změn záznamu probíhá mazání prvku pouze formou změny atributu a prvek zůstává i nadále uložen v systému.  Synchronizační mechanismy a architektura systému  umožní adekvátní propsání do všech řízených systémů. |
| 1.6 | Systém podporuje rozdílovou i celkovou synchronizaci změn do/z řízených informačních systémů a adresářové služby. | Napojení na zdrojový systém probíhá neinvazivní formou, a tudíž je zatížení zdrojového systému napojením na cIDM minimální a zátěž na zdrojový systém by tak měla být co nejmenší.  Vlastní napojení je realizováno přírůstkovou synchronizací nebo exportem celé databáze uživatelů. Může být realizováno pomocí standardního rozhraní např. LDAP nebo cestou importu souborů ve formátu CSV, XML, JSON případně využitím webové služby.  Dalším ze způsobů napojení je přímý přístup do |

|  |  |  |
| --- | --- | --- |
|  |  | databáze realizované pomocí ODBC driveru případně pomocí jiných dostupných konektorů.  Pro Active Directory disponuje cIDM konektorem umožňujícím základní práci s daty uživatele jako je úprava informací o uživateli, změna hesla a jeho obnova. Umožnuje také správu skupin v Active  Directory a správu vazeb mezi uživatelem a skupinou. |
| 1.7 | Systém umožňuje přebírání zdrojových dat, publikace a změny dat z různých referenčních zdrojů ve stávajících, modernizovaných a nově pořizovaných informačních systémech včetně případného vytvoření integračního rozhraní na straně nástroje ve spolupráci s jejich dodavateli/výrobci, zejména:   1. interní systém organizace pro řízení lidských zdrojů = referenční zdroj zdravotnických a nezdravotnických pracovníků organizace a pracovně- právní organizační struktury 2. nástroj pro správu životního cyklu kvalifikovaných certifikátů a prostředků pro vytváření kvalifikovaných elektronických podpisů dle eIDAS = referenční zdroj identifikátorů bezkontaktních čipových karet   Konkrétní způsob vzájemného předávání a správy referenčních dat mezi systémy budou předmětem návrhu schváleného odpovědnými pracovníky zadavatele. | Jako zdrojový systém je chápán systém udržující informace o různých entitách v rámci organizace. Těmi mohou být zaměstnanci, dodavatelé, zákazníci, auditoři, systémy hardware a další. Zdrojové systémy mohou dále poskytovat informace o organizační struktuře a vztazích jednotlivých entit k organizační struktuře.  Napojení na zdrojový systém probíhá neinvazivní formou, a tudíž je zatížení zdrojového systému napojením na cIDM minimální a zátěž na zdrojový systém by tak měla být co nejmenší.  Vlastní napojení je realizováno přírůstkovou synchronizací nebo exportem celé databáze uživatelů. Může být realizováno pomocí standardního rozhraní např. LDAP nebo cestou importu souborů ve formátu CSV, XML, JSON případně využitím webové služby. Dalším ze způsobů napojení je přímý přístup do databáze realizované pomocí ODBC driveru případně  pomocí jiných dostupných konektorů. |

|  |  |  |
| --- | --- | --- |
|  | IdM může být referenčním zdrojem dat (např. uživatelských účtů, evidence a přiřazení jednotlivých rolí v rovině finančních zdrojů pro konkrétní zdroje financování, evidenci souhlasů s veřejným použitím fotografie osoby, evidence komisí a jejich členů, evidenci externích osob,  dodavatelů a servisních účtů). | Systém cIDM slouží v rámci organizace jako referenční zdroj pro veškeré entity a pomocí standardního rozhraní je zpřístupňuje oprávněným systémům uvnitř i vně organizace. |
| 1.8 |  | Uchování informací o entitách je realizováno primárně v interní databázi v rámci platformy IRIS for Health s možností uchovávat v zabezpečené podobě uživatelská hesla a poskytovat základní funkcionality založení účtu, jeho smazání, obnovy a změny hesla. V rámci uchování informací o identitách je možné také evidovat rozšiřující informace jako jsou: |
|  |  | * Demografické údaje o identitě jako jsou:   + jméno,   + příjmení,   + datum narození,   + tituly   + rodné číslo, * fotografie uživatelů, * kontaktní informace (e-mail, telefonní číslo) * jejich účty v napojených systémech obsahující například Identifikátory (GS1 kód, Osobní číslo, Login), |

|  |  |  |
| --- | --- | --- |
|  |  | * včetně informací uložených na elektronických kartách, včetně přístupových karet. Čip z karty a další * certifikáty (bankovní, a dalších autorit, certifikáty osobní, komerční atd.) * souhlasy (GDPR, fotografie, ...)   Systém umožňuje uchovávání všech typů entit, které v rámci organizace mohou přistupovat k zabezpečeným zdrojům. Mezi hlavní patří:   * Uživatelé * Dodavatelé * Zákazníci * Servisní účty systémů * Hardware   ... |
| 1.9 | Systém umožňuje vytvoření uživatelského účtu včetně vygenerování počátečního hesla s vynucením jeho změny při prvním použití po založení uživatele v referenčním zdroji (např. předání přihlašovacích údajů zaměstnanci na personálním oddělení v rámci nástupu do zaměstnání). | Zdrojem entit může být pro cIDM jeden nebo více externích systémů, který organizace využívá pro stávající správu. Typicky pro správu uživatelů připadá v úvahu napojení personálního systému, nebo CRM systému. Systém také uchovává účty, které nejsou  evidované ve výše zmíněných systémech a jsou |

|  |  |  |
| --- | --- | --- |
|  |  | potřebné pro provoz infrastruktury a její správu. Tyto entity lze spravovat přímo v cIDM.  V rámci GUI cIDM lze provádět příjem pracovníka společně se založením jeho uživatelského účtu. |
| 1.10 | Systém umožňuje provoz samoobslužného portálu pro obnovu zapomenutého hesla. | Uživatel má na přihlašovací stránce web aplikace  možnost sám si změnit svoje aktuální přístupové heslo do systému |
| 1.11 | IdM bude poskytovat možnost zadání údajů pro samoregistrující uživatele. | Aplikace obsahuje možnost založení účtu pro nového uživatele procesem tzv. samoregistrace. Uživatel sám na příslušné stránce zadá základní informace o svojí osobě a vygeneruje si přístupové údaje (jméno a heslo). Následně se automaticky spustí proces pro schválení této registrace a pro přidělení  odpovídajících interních rolí uživateli. |
| 1.12 | IdM bude otevřený pro integrace na jiné budoucí datové základny. | Nabízené řešení obsahuje konfigurační nástroje pro vytvoření konektorů pro připojení libovolného počtu  integrovaných systémů a datových zdrojů |
| 1.13 | Systém umožní správu rolí (RBAC) a průnik vícenásobných rolí (různé úvazky v různých odděleních/účast na různých grantech) včetně možnosti samoobslužné žádosti o určitou roli, řešení expirace a prodlužování přístupu (např. u ručně zakládaných externistů). | Oprávnění v rámci systému jsou založena na RBAC (Role-Based Access Control) a jednotlivým entitám jsou přiřazována oprávnění formou rolí. Pro možnost efektivnější správy rolí v organizační struktuře jsou definována typová pracovní místa, která definují obecná oprávnění včetně jejich hierarchií pro jednotlivé skupiny uživatelů. |

|  |  |  |
| --- | --- | --- |
|  |  | Oprávnění mohou mít definována vlastní časová omezení, nad rámec životního cyklu přiřazeného prvku organizační struktury.  Na organizační strukturu jsou pomocí jednoho či více pracovních vztahů navázány jednotlivé entity, které mohou reprezentovat jak uživatele, správce, systémy nebo hardware. Entity v rámci svého pracovního vztahu nabývají definovaná oprávnění v napojených systémech a ta jim mohou být přiřazena i nad rámec jejich základních pracovních vztahů.  V rámci GUI cIDM je možné žádat o přidělení a prodloužení oprávnění. |
| 1.14 | IdM podporuje neomezenou hierarchii rolí včetně možnosti tvorby katalogu rolí a podpora řízení životního cyklu rolí. | Pro možnost efektivnější správy rolí v organizační struktuře jsou definována typová pracovní místa, která definují obecná oprávnění včetně jejich hierarchií pro jednotlivé skupiny uživatelů.  Oprávnění mohou mít definována vlastní časová omezení a jsou také závislá na životním cyklu přiřazeného prvku organizační struktury. |
| 1.15 | IdM podporuje možnost provádění inventury přístupových práv k  zabránění kumulování většího množství práv jedné osoby v průběhu času včetně vynuceného předschválení rolí s eskalačním mechanismem. | Systém obsahuje generátor reportů pro různá vstupní kritéria a podmínky. |

|  |  |  |
| --- | --- | --- |
|  |  | Definice role obsahuje, kromě jiných parametrů, jako je například zařazení role do skupiny vzájemně se vylučujících rolí u jedné entity, také možnost přidat roli do skupiny rolí, které je nutné společně schvalovat vyšší instancí. To zajišťuje eskalaci schvalování rolí,  pokud se definovaným způsobem kumulují. |
| 1.16 | IdM poskytuje podporu principu „čtyř očí“, tedy je možné kontrolovat, že osoba s přidělenou specifickou rolí nemůže mít zároveň přidělena jinou specifickou roli (např. příkazce operace a správce rozpočtu stejného zdroje financování v rámci vnitřního kontrolního systému nemůže být  tatáž osoba). | Entita (uživatel) může mít přiřazený seznam rolí, které uživateli nelze v aplikaci přiřadit. |
| 1.17 | IdM obsahuje podporu kontrolních mechanismů na byznys vrstvě, která umožní sledovat chybějící oprávnění (např. příkazce operace finančního zdroje ukončí pracovní poměr a bez nominace jiného příkazce operace nelze finační zdroj čerpat). | Správa rolí v napojených systémech umožňuje definovat role s povinným přiřazením k entitě.  V kombinaci s příslušnými reporty lze získat přehled  o přiřazených resp. nepřiřazených rolích u evidovaných entit. |
|  | IdM umožňuje vytváření více typů účtů (více uživatelských jme, resp. identit) k jedné fyzické osobě (např. běžný a administrátorský účet). IdM bere tento fakt v potaz. | Systém umožňuje uchovávání všech typů entit, které v rámci organizace přistupují k zabezpečeným zdrojům. Mezi hlavní patří: |
| 1.18 |  | * Uživatelé * Dodavatelé * Zákazníci * Servisní účty systémů * Hardware |

|  |  |  |
| --- | --- | --- |
| 1.19 | IdM umožňuje reporting a vytváření auditní stopy operací nad činností IdM a oprávněných uživatelů (historické změny v uživatelských účtech, historické změny v uživatelských rolí, schvalování apod.). | Všechny změny v IDM, tedy jak změny definic, tak změny v záznamech o entitách a přiřazení vztahů jsou zaznamenány pro účely auditování. Auditní záznam má všechny náležitosti potřebné pro identifikaci změn  - časové razítko, identifikaci původce změny, atd.  Z auditního logu lze pořizovat jednoduché reporty. Složitější analýzy jsou možné pomocí analytických  dotazů v SQL. |
| 1.20 | IdM spravuje identity v řízených informačních systémech prostřednictvím vlastních konektorů, které jsou využívány rozhraním daného systému (např. CSV, ODBC, LDAP, REST, SOAP apod.) bez nutnosti instalace pomocné komponenty (agenta) do řízeného informačního systému/adresářové služby; kromě plně automatizovaných konektorů (čtení/zápis do/z informačního systému) IdM podporuje plně manuální konektor (notifikuje odpovědné osoby o nutnosti ruční změny  v informačním systému) a poloautomatický konektor (notifikuje odpovědné osoby o nutnosti ruční změny, ale zároveň umožňuje manuální načtení stavu v informačním systému pro kontrolu). | Komunikace s napojenými systémy probíhá pomocí standardního rozhraní, jako alternativní způsob napojení systémů lze vytvořit konektor pro jednotlivé aplikace, pomocí kterých budou systémy konzumovat změny v oprávněních, nebo aktualizovat celou databázi uživatelů a jejich oprávnění.  Konektor může být realizovaný jako:   * napojení na API systému, přes které je možné v systému zakládat uživatele a jejich oprávnění * vytvoření exportu pro daný systém, který si následně zpracuje.   Systém disponuje možností vytvořit libovolný konektor. |
|  |  | Konektory pro systémy, které nejsou schopny  konzumovat standardní rozhraní, přijímat informace o entitách pomocí vystavení webové služby ani |

|  |  |  |
| --- | --- | --- |
|  |  | zpracování exportu musí být realizovány  operátorem/správcem pro daný systém. Jejich vlastní realizace záleží na dostupných možnostech systému. |
| 1.21 | Webové rozhraní pro žádost o přidělení práv prostřednictvím IdM má ovládání přizpůsobené různým dotykovým zařízením (responzivní design pro samoobslužnou část) a platformám (iOS, Android atd.), přístup do klientské části je nezávislý na operačním systému přistupujícího klienta a možný prostřednictvím webového prohlížeče bez nutnosti instalace dalšího SW (aplikací, modulů, appletů či knihoven) tj. zejména bez použití např. ORACLE Java, Microsoft Silverlight, Adobe Flash. | Grafické rozhraní provisioning systému je realizováno pomocí single page aplikace využívající technologie Angular (v aktuální verzi) a umožňuje současnou práci více uživatelů.  Responzivní web design aplikace zajišťuje optimalizaci grafického uživatelského rozhraní pro různé druhy zařízení (tablet, mobilní telefon, notebook nebo PC) a jeho univerzální použitelnost ve všech standardních prohlížečích. |
| 1.22 | Autentizace/autorizace uživatelů k webovému rozhraní IdM bude připraveno na využití SSO webového portálu. | Přístup do systému je zabezpečen pomocí framework OpenID Connect založeného na OAuth2  Grafické rozhraní je připraveno komunikovat s SSO bránou založenou na protokolu SAML. |
| 1.23 | Systém musí být připraven na napojení na Národní identitní autoritu. | Systém disponuje konektory pro připojení k identitním autoritám a může být napojen i na prostředí NIA, jakmile toto bude připravené poskytovat  odpovídající online služby. |

### Funkční požadavky

|  |  |  |
| --- | --- | --- |
| **Číslo požadavku** | **Popis požadavku** | **Způsob naplnění požadavku - popis funkce, standardní součást produktu nebo vývoj na klíč** |
| 2.1 | IdM disponuje záznamem vybraných operací nad identitami v auditním logu, přičemž historie změn bude zahrnovat i autora změny. | Všechny změny identit (přidání nové, změny existující, smazání) jsou zaznamenány pro účely auditování. Auditní záznam má všechny náležitosti - časové razítko, identifikaci původce  změny, atd. |
| 2.2 | Systém obsahuje profily uživatelů, k nimž jsou přiřazována příslušná oprávnění. | Na organizační strukturu jsou pomocí jednoho či více pracovních vztahů navázány jednotlivé entity, které mohou reprezentovat jak uživatele, správce, systémy nebo hardware. Entity v rámci svého pracovního vztahu nabývají definovaná oprávnění v napojených systémech a ta jim mohou být přiřazena i nad rámec jejich základních pracovních vztahů. |
| 2.3 | Systém umožňuje vícekriteriální vyhledávání a ukládání filtrů. | Systém obsahuje možnost definice a uložení různých filtrů  pro vyhledávání. |
| 2.4 | Systém umožňuje omezení přístupů uživatelů do různých částí evidovaných dat. | Řízení přístupu je založené na oprávněních v aplikaci, která umožňují realizaci případů užití. Kombinace jednotlivých případů užití je zastřešená rolí v systému s nastavitelným rozsahem. Řízení přístupu je v souladu s bezpečnostními standardy OpenId Connect. |
| 2.5 | Systém umožňuje přenášení oprávnění z osoby na osobu (jeden uživatel bude dělat totéž, co předchozí). | Pro pracovní vztahy je možné definovat zastupitelnost, na dobu určitou a na dobu neurčitou, po kterou oprávnění z jednoho pracovního vztahu entity přecházejí na pracovní vztah jiné entity. |

|  |  |  |
| --- | --- | --- |
| 2.6 | Systém umožňuje kopírování oprávnění mezi prostředími  (produkční a testovací). | Systém umožnuje kopírování oprávnění mezi jednotlivými  prostředími. |
| 2.7 | Systém udržuje historii provedených změn u pracovníků s možností zobrazení stavu ve vybraném čase (podle data je možné ukázat, jaké bylo nastavení k příslušnému datu), které musí být shodné se standardním zobrazením dat. | Pro aktuální stav entity (člověk nebo oprávněné zařízení) disponuje IDM standardním zobrazením, které ukazuje všechna oprávnění se všemi charakteristikami, které entita právě vlastní. V tomtéž zobrazení lze zobrazit stav k zadanému datu v  minulosti. |
| 2.8 | Systém uchovává informace o odstraněných pracovnících  (neaktivní účty s posledním platným nastavením). | Mazání v systému probíhá označením jednotlivých prvků jako  smazanými pro uchování úplné historie. |
| 2.9 | IdM musí umožnit reagovat na události změny organizační struktury, změny oprávnění nebo změny vlastností identit tak, že odešle relevantní informaci formou e-mailu. Konfigurace událostí a reakcí na ně musí být uživatelsky definovatelné. | Systém disponuje konfigurovatelnou funkcionalitou informačních textů. V návaznosti na události v rámci životního cyklu entity a organizační struktury je entitě vygenerován informační text, který jí seznámí s rozsahem oprávnění v jednotlivých informačních systémech, která jsou jí v rámci cIDM definována. Tento text je následně entitě odeslán do její e-mailové schránky. Stejně tak v případě změny v oprávněních, nebo změně vztahu k organizační struktuře je entita o takové změně informována. |
|  |  | Vlastní provedení notifikace je konfigurovatelné pro příjemce, původce notifikace a pro systém, který je změnou v oprávněních  dotčen. |
| 2.10 | Systém umožňuje provádění kontroly konzistence dat skutečného stavu v adresářové službě a řízených informačních systémech oproti očekávanému stavu v IdM (zejména kvůli odhalení změn, které byly do adresářové služby nebo řízených | IDM je napojeno na adresářovou službu a řízené informační systémy prostřednictvím svých integrační komponent. Pokud to adresářová služba a/nebo řízený systém umožňuje a požaduje, lze konfigurační data synchronizovat, kontrolovat konzistenci,  případně posílat upozornění na změny. |

|  |  |  |
| --- | --- | --- |
|  | informačních systémů zaneseny mimo IdM např. ručním  zásahem administrátora). |  |
| 2.11 | Systém podporuje mapování atributů mezi různými řízenými informačními systémy a adresářovou službou – převod hodnot mezi různými atributy včetně možnosti algoritmizovat způsob převodu pomocí transformační logiky/skriptovacího jazyka (např. slučování/rozdělování atributů do jednoho/více atributů, textové úpravy hodnot, odstranění diakritiky, definici podmínek včetně absolutního a relativního času – např. smazání účtu až po x dnech od ukončení pracovního poměru/zablokování) | IDM je napojeno na adresářovou službu a řízené informační systémy prostřednictvím své integrační platformy. Tím zajišťuje jak maximální přizpůsobení potřebám a možnostem napojeného systému, tak pružné procesní řízení způsobu a smyslu komunikace, včetně možnosti přidávání časových prodlev. Pro konverzi vstupně/výstupních dat lze využít jak zabudované transformační mechanismy, tak výkonný skriptovací jazyk. Změny kódování, práce s diakritikou, úpravy a slučování či  rozdělování hodnot ve více polích jsou samozřejmostí. |
| 2.12 | Systém zahrnuje uživatelské rozhraní pro manuální editaci vybraných informací z uživatelského profilu, např. uživatelské heslo. | Uživatel má na přihlašovací stránce web aplikace možnost sám si změnit svoje aktuální přístupové heslo do systému. Po přihlášení do systému má uživatel možnost upravit některé údaje  svého profilu. |
|  | Systém umožňuje jednotnou evidenci maticové organizační struktury (organizační – pracovně-právní a projektové/grantové). | **Správcovský modul** umožňuje centrální pohled na oprávnění a jejich nastavování v souladu s oprávněními správce v systému. Mezi případy užití pro správcovský modul patří: |
| 2.13 |  | * Zobrazení organizační struktury * Úpravy v rámci organizační struktury. * Nastavování bezpečnostní politiky pomocí definice typových pracovních míst. * Přidělení typových pracovních míst k jednotlivým pracovním zařazením. * Definice filtrů pro automatickou aplikaci typového   pracovního místa. |

|  |  |  |
| --- | --- | --- |
|  |  | * Vyhledání entity. * Definice filtrů pro vyhledávání * Zobrazení informací o entitě. * Prohlížení oprávnění jednotlivých entit. * Založení entity * Editace profilu entity. * Úpravy individuálních oprávnění entity * Nastavení sdílených adresářů v AD Správa napojených systémů * Správa rolí v napojených systémech (vzájemně se vylučující role, skupiny rolí podléhající eskalovanému schválení, povinné přiřazení) * Spouštění aktualizace systému * Tisk informačního textu pro nastupujícího zaměstnance * Práce se zálohou * Generování reportů |
| 2.14 | V systému lze provádět nastavení přístupových práv do aplikací s využitím profilů, a přístupových práv k datům na souborovém systému v prostředí Windows. | Pro Active Directory disponuje cIDM konektorem umožňujícím základní práci s uživatelem - úpravy informací o uživateli, změnu hesla a jeho obnovu. Umožnuje správu skupin v Active Directory a správu vazeb mezi uživatelem a skupinou.  cIDM umožňuje správu přístupu ke sdíleným síťovým prostředkům v rámci systému Windows pro jednotlivé uživatele v rámci konektoru na Active Directory. |

|  |  |  |
| --- | --- | --- |
| 2.15 | Systém umí generovat výstupy pro podporu tvorby telefonního seznamu organizace ve formě webových služeb, exporty dat do XML, grafické znázornění organigramu organizace. | Výstup pro podporu tvorby telefonního seznamu je jedním ze standardních reportů IDM a je k dispozici i prostřednictvím webové služby.  Export veškerých dat do XML je standardní funkcionalitou IDM IDM obsahuje také možnost grafického zobrazení organigramu a strukturovaného textový popisu celé dané organizační  hierarchie či její vybrané části. |
| 2.16 | Systém odesílá e-mailovou notifikaci definované osoby  v případě vytvoření, přesunutí nebo odstranění. | IDM informuje o změnách v oprávněních konfigurovatelnou  emailovou notifikací, viz také bod 2.9 |
| 2.17 | Systém odesílá e-mailovou notifikaci zastupující osobě v případě vytvoření zástupu. | cIDM informuje o změnách v oprávněních i v případě  vytvoření zástupu konfigurovatelnou e-mailovou notifikací, viz také bod 2.9 |
| 2.18 | Systém poskytne rozhraní pro import uživatelských rolí z integrovaných systémů. | Strukturu rolí řízených systémů je možné do cIDM importovat ze souborů formátu CSV nebo XML. |
| 2.19 | Systém umožní evidenci uživatelů, kteří nebudou synchronizováni do centrální adresářové služby. | Zdrojem entit může být pro cIDM jeden nebo více externích systémů, které organizace využívá pro stávající správu. Typicky pro správu uživatelů připadá v úvahu napojení personálního systému, nebo CRM systému. Systém také uchovává účty, které nejsou evidované ve výše zmíněných systémech a jsou potřebné pro provoz infrastruktury a její správu. Tyto entity lze spravovat přímo v cIDM a lze u nich nastavit příznak, zda mají být propisovány pomocí konektroů do napojených systémů. |
| 2.20 | Systém musí umožnit evidenci všech aplikací provozovaných v organizaci, a to až na úroveň jednotlivých modulů. | IDM udržuje evidenci všech “domén” tedy aplikací, modulů, či  jiných entit, ke kterým je možné zřídit přístup. Aplikace mají v evidenci jak (nepovinnou) vazbu na organizační strukturu, tak |

|  |  |  |
| --- | --- | --- |
|  |  | řadu definičních parametrů. K aplikaci jsou také evidovány její  jednotlivé moduly, pokud je má. |
| 2.21 | Systém umožní fulltextové vyhledávání v aplikaci pro vybrané vlastnosti evidovaných objektů. | V rámci GUI cIDM je možné fulltextově vyhledávat přes dostupné atributy entit pomocí tzv. chytrého vyhledávacího okna. |
| 2.22 | Systém umožní filtrování v seznamech (seznam aplikací,  seznam osob, seznam organizačních jednotek apod.). | Systém obsahuje možnost definice a uložení různých filtrů  pro vyhledávání v různých oblastech systému. |

### Technické požadavky

|  |  |  |
| --- | --- | --- |
| **Číslo požadavku** | **Popis požadavku** | **Způsob naplnění požadavku - popis funkce, standardní součást produktu nebo vývoj na klíč** |
| 3.1 | GUI Systému podporuje aktuální verze prohlížečů:   * Microsoft Internet Explorer * Microsoft Edge * Google Chrome (desktop, Android) * Mozilla Firefox | Responzivní web design aplikace zajišťuje optimalizaci grafického uživatelského rozhraní pro různé druhy zařízení (tablet, mobilní telefon, notebook nebo PC) a jeho univerzální použitelnost ve všech standardně používaných prohlížečích. |
|  | Safari pro iOS/iPadOS |  |
| 3.2 | Systém bude obsahovat nápověda přímo v aplikaci (formulářová a položková nápověda). | GUI prostředí aplikace obsahuje krátkou nápovědu u jednotlivých položek formuláře. Pro popis činnosti a dalších souvisejících informací je určena celostránková textová  nápověda. |

|  |  |  |
| --- | --- | --- |
| 3.3 | Součástí dodávky IdM je kompletní uživatelská a  administrátorská dokumentace v elektronické verzi. | cIDM obsahuje uživatelskou i administrátorskou dokumentaci  v elektronické podobě |
| 3.4 | IdM bude obsahovat obecné zdokumentované rozhraní pro vstup dat z personálního systému včetně importu nadřízenosti a podřízenosti jednotlivých rolí, budov organizace a kontaktů  pracovníků (telefonní čísla, e-maily, místnosti). | Rozhraní pro import dat z personálního systému bude dodáno v rámci Etapy I |
| 3.5 | Objednatel požaduje poskytnutí zdrojového kódu ke konektorům a programovým úpravám, které byly v rámci  dodávky vytvořeny/upraveny pro potřeby Objednatele. | Veškeré zdrojové kódy k částem systému dodaným na základě požadavku objednatele jsou automatickou součástí dodávky. |