1. Popis nabízeného technického řešení (popis cílového stavu a funkčních vlastností)
   1. Obecné požadavky
      * 1. Uchazeč v rámci zakázky navrhne:
           1. způsob nasazení a zavedení personálního a mzdového systému včetně převodu relevantních údajů ze stávajícího systému a napojení na související systémy.
           2. způsob nasazení a zavedení systému pro správu identit včetně propojení (integrace) s hlavními informačními systémy
           3. způsob nasazení a zavedení systému pro správu provozní (nezdravotní) dokumentace
        2. Uchazeč v rámci zakázky provede po schválení návrhů z předchozího bodu jejich realizaci.
        3. Zadavatel při výstavbě, správě a provozu ICT technologií striktně dodržuje hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.
        4. Bude využito stávajících prostředků a používaných technologií.
        5. Uchazeč bude při implementaci respektovat provozní řád Zadavatele, vítězný Uchazeč bude s provozním řádem seznámen před podpisem Smlouvy o dílo.
        6. Veškerá dokumentace vytvořená v rámci veřejné zakázky, bude zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, PDF) používaných Zadavatelem na datovém nosiči a 1x v papírové formě. Papírová forma bude logicky a věcně strukturovaná, bude připravena pro použití (např. provozní dokumentace ICT ve formě vhodné pro použití administrátory v serverovně). Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena Zadavatelem.
   2. Specifické požadavky K1 – Správa identit
      * 1. Systém pro správu identit (Identity management – IDM) bude koncipován jako ústřední systém správy ICT. Bude kopírovat organizační strukturu Zadavatele a umožní automatizaci úkonů spojených se správou identit v informačních systémech Zadavatele a zvýší úroveň kybernetické bezpečnosti.
        2. Automatizací správy identit dojde k odstranění nebo alespoň významnému omezení rutinních činností správců systémů spojených se správou identit a dále ke zrychlení reakcí na změny v organizace (např. změny oprávnění v systémech při změně pozice zaměstnance), snížení chybovosti způsobené ručním zadáváním údajů do systémů a/nebo nedodržením procesů (např. včasným nenahlášením odchodu zaměstnance všem správcům systémů nedojde včas nebo vůbec ke zrušení přístupových účtů zaměstnance) a získání okamžitého detailního přehledu o stavu identit a jejich oprávnění v systémech Zadavatele.
        3. Na IDM budou navázány hlavní informační systémy Zadavatele – personalistika, docházka, groupware, informační systémy NIS a PACS, systém pro správu požadavků, systém pro správu a evidenci majetku i nově pořizovaný systémy správy dokumentů. IDM tak vytvoří jeden autorizovaný zdroj informací ohledně uživatelů a jejich práv přístupů k jednotlivým systémům, tím bude současně provedena konsolidace identit, která je nezbytná pro realizaci budoucí uvažovaných projektů spojených s identitami – realizaci nařízení Evropské unie č. 910/2014 eIDAS o elektronické identifikaci a důvěryhodných službách pro elektronické transakce.
        4. IDM poskytne uživatelům základní službu „Přístup k systémům synchronizovaným s IDM“. Tato služba je realizována v procesech přístup do systému, přístup k aplikacím synchronizovaným s IDM apod. V případě, že jsou poskytovány aplikace externím subjektům, zajistí IDM přihlášení k aplikacím pro externí subjekty. V IDM budou vytvářeny role a těm se přidělovány oprávnění pro jednotlivé aplikace. Role budou naplňovány konkrétními uživateli. Tímto způsobem mohou být definovány role pro všechny zaměstnance a nový zaměstnanec automaticky při nástupu získá všechna potřebná oprávnění, a naopak při ukončení pracovního poměru bude zřejmé, že mu všechna přístupová práva byla odebrána.
        5. Součástí IDM bude detailní logování prováděných změn pro možnost zjištění uživatelských oprávnění v libovolném času v minulosti (od nasazení systému).
        6. Implementace systému bude provedena v souladu s § 19 Nástroj pro řízení přístupových oprávnění Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

|  |  |  |
| --- | --- | --- |
| **Komodita K1 - Správa identit** | | |
| **Část** | **Parametr** | **Popis** |
| **Systém pro správu identity (Identity management - IDM)** | Základní funkce | Systém pro správu identit - Identity management (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi. |
|  | Licence | Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). |
| **AC IDENTITA** | Počet spravovaných uživatelů je 2100. |
|  | Škálovatelnost | Systém umožňuje zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. |
|  | Evidence aplikací a rolí | Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby. |
|  | Uživatelské role | Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS. |
|  | Historizace | Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti. |
|  | Automatizace | Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). |
|  | Logování SIEM | Systém poskytuje auditní logy ve formátu vhodném pro systém typu SIEM (Security Information and Event Management) |
|  | Logování systému | Systém obsahuje logování následujících typů událostí: |
|  | - události systému (aplikační log) |
|  | - změny entit evidovaných systémem a změny konfigurace systému (auditní log) |
|  | - synchronizace s napojenými systémy (synchronizační log) |
|  | - odeslané notifikace a upozornění (notifikační log) |
|  | Správa identit | Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury. |
|  | Systematizovaná místa | Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu. |
|  | Podpora eIDAS | Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. |
|  | Vysoká dostupnost | Systém je možno nasadit na více serverů v režimu vysoké dostupnosti. |
|  | Požadavky na portál - obecné | IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. |
|  | Podpora mobilních zařízení | Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno) |
|  | Správa referenčních objektů | Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát. |
|  | Referenční objekty | Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity |
|  | Zabezpečení referenčních objektů | Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů |
|  | Rozšiřující atributy | Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM. |
|  | Přehledné zobrazení | Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit). |
|  | Vyhledávání - diakritika | Portál bude umožňovat vyhledávat i bez diakritiky (zadání Parizek vyhledává i Pařízek apod.) |
|  | Správa certifikátů | Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti. |
|  | Obrázky | Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie. |
|  | Přesun identit | Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními. |
|  | Kopírování rolí | Systém umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy. |
|  | Ochrana proti chybám | Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod). |
|  | Aktivní uživatelé | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem |
|  | Slučování identit | Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů. |
|  | Export údajů | Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu |
|  | Filtrování | Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití. |
|  | Správa oprávnění | Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) |
|  | Granularita oprávnění | Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět. |
|  | Oprávnění k atributům | Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů. |
|  | Kontextový výběr | Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky. |
|  | Správa licencí | IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow. |
|  | Časová omezení | IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere. |
|  | Vícenásobné vazby | Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. |
|  | Přehled rolí | Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role. |
|  | Přehled dědičností | IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu. |
|  | Skupiny | IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. |
|  | Zastupitelnost | IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce. |
|  | Delegování oprávnění | Možnost delegování administrátorských práv. |
|  | Správa osobních údajů | IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací. |
|  | Osobní údaje | IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům. |
|  | Osobní údaje - automatizace | IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů. |
|  | Obnovení hesla | IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. IDM je možné na SMS bránu či službu napojit). Rozhraní bude umožňovat i běžnou změnu hesla (bez resetu). |
|  | Žádosti | IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení. |
|  | Externí subjekty | IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin. |
|  | Kontextový výběr | Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat. |
|  | Individualizace | IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně. |
|  | Workflow | Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: |
|  | - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným |
|  | - Možnost sledování stavu svých požadavků uživateli |
|  | - E-mailové upozornění schvalovatele na požadavek ke schválení |
|  | - Přehled úloh ke schválení pro každého schvalovatele |
|  | - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění |
|  | - Podpora vícekrokového schvalování |
|  | - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) |
|  | - Správce IDM může pracovat se všemi úlohami |
|  | - Možnost větvení pro ošetření výjimek vzniklých při schvalování |
|  | - Řešení zastupitelnosti |
|  | - Eskalace - upozornění při překročení termínu splnění |
|  | - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů |
|  | Workflow - sledování | Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazní workflow aktivity diagram, BPMN nebo Archimate |
|  | Upozornění | IDM zajistí zasílání konfigurovatelných emailových upozornění pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. |
|  | Včasná upozornění | Upozornění na vypršení časových termínů bude možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně. |
|  | Šablony upozornění | Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám bude možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony bude umožňovat vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu. |
|  | Kontext upozornění | Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd. |
|  | Logování | Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu. |
|  | Důvěryhodnost logování | Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM. |
|  | Provozní stav | Kumulovaný online přehled o aktuálním stavu hlavních částí systému a případných chybách - min. chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu workflow. |
|  | Auditní report | IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. |
|  | Auditní report - výběr | Identity pro generování auditního reporty bude možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů. |
|  | Reporty uživatelů | Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru. |
|  | Reporty - zasílání | Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel. |
|  | Reporty - historie | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. |
|  | Reporty - porovnání | Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu. |
|  | Webové služby (WS) | IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. |
|  | Standardy WS | Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. |
|  | Bezpečnost WS | Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. |
|  | Logování WS | Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu |
|  | Služby rozhraní WS | Rozhraní bude poskytovat minimálně následující služby: |
|  | - Získání organizační struktury |
|  | - Získání hierarchie systematizovaných míst |
|  | - Získání seznamu identit |
|  | - Získání nadřízené osoby pro daného zaměstnance |
|  | - Získání seznamu funkcí / rolí |
|  | - Získání seznamu uživatelů dané aplikace |
|  | - Získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci |
|  | - Zápis seznamu funkcí do IDM |
|  | - Zápis certifikátů do IDM |
|  | - Zápis a změna identit |
|  | Synchronizace | Ruční i automatické spuštění synchronizací s propojenými systémy. |
|  | Synchronizace - simulace | Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu. |
|  | Simulace - průběh | Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě. |
|  | Synchronizace - režimy | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): |
|  | - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému |
|  | - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. |
|  | - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu. |
|  | - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému. |
|  | - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. |
|  | - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala. |
|  | Synchronizace - správa | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu. |
|  | Obecné konektory | Vestavěné obecné konektory pro správu identit v napojených systémech: |
|  | - konektor pro spouštění CMD příkazů |
|  | - konektor pro práci s CSV soubory |
|  | - konektor pro práci s databází Microsoft SQL |
|  | - konektor pro napojení na SOAP a REST webové služby |
|  | - konektor pro napojení na LDAP server s podporou LDAP v3 |
|  | Speciální konektory | IDM bude obsahovat konektor umožňující správu virtuálních aplikací. Požadavky na správu identit ve virtuálních aplikacích bude IDM předávat e-mailem správcům odpovídajících reálných aplikací. Správci potvrdí splnění požadavku zpět do IDM. Uvedeným systémem budou řízeny identity v aplikacích, které nelze nebo není ekonomicky efektivní integrovat s IDM pomocí obecných nebo aplikačních konektorů. |
|  | Aplikační konektory | IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet a spravovat uživatelské účty a jejich oprávnění včetně souvisejících operací potřebných pro plnou automatizaci správy identit v daném systému (řízení členství ve skupinách, přiřazení rolí, správa metadat): |
|  | - Microsoft Active Directory |
|  | - ekonomický systém Helios Green (Asseco) |
|  | - NIS tj. nemocniční informační systém) Fons Enterprise (Stapro) |
|  | - Laboratorní systém OpenLims (Stapro) |
|  | - PACS - MARIE PACS (OR-CZ) |
|  | - groupware IceWarp Mail Server, včetně vytváření schránek (IceWarp) |
|  | - docházkový systém (IVAR) |
|  | - Service desk (Alvao) |
|  | - Asset management (Alvao) |
|  | - DMS - Komodita K2 |
|  | Zdrojový systém | IDM bude napojeno na personální systém Avensio (Alfa software). Z personálního systému budou načítány údaje o organizační struktuře, pracovních místech a funkcích, osobách a tyto údaje budou pro IDM sloužit jako zdrojové |
|  | Záruka | 12 měsíců včetně nároku na opravné verze |

* 1. Specifické požadavky K2 – Správa provozních dokumentů
     + 1. Systém správy dokumentů (Document management system - DMS) bude navržen jako webový prostor (intranet) pro interní využití s důrazem na jednoduchost a rychlost použití, s možností dále toto řešení rozvíjet a dotvářet vlastními silami zadavatele.
       2. Systém vytvoří podmínky pro zavedení automatizovaného zpracování dokumentů a souvisejích procesů včetně jejich schvalování. Nativní vlastností řešení bude možnost parametrizace systému včetně tvorby wokflow – pro pozdější rozšiřování a úpravy systému.
       3. Systém umožní rychlé vyhledávání. Zadáním a potvrzením hledaného slova či fráze se prohledá uložená dat a zobrazí se relevantní výsledky.
       4. Systém bude využívat a poskytovat data ekonomickému systému HELIOS Green v rozsahu funkčnosti požadované povinnými parametry
       5. Systém bude integrován se systémem K1 pro správu identit pro zajištění automatizace správy identit (uživatelských účtů) a stávajícm groupwarovým systémem tak, aby uživatelé byli informováni o svých úkolech (např. požadavek na schválení).

|  |  |  |
| --- | --- | --- |
| **Komodita K2 - Správa provozních dokumentů** | | |
| **Část** | **Parametr** | **Popis** |
| **Systém pro správu dokumentů** | Základní funkce | DMS systém (Document management systém - dále jen DMS nebo systém) - systém koncipovaný jako portál dostupný prostřednictvím webového prohlížeče, obsahující dále uvedené aplikace či moduly a funkce. |
|  | **Aplikace - moduly** | |
| **Funkční rozšíření stávajícího řešení ALVAO** | Smlouvy | Obsahuje podklady o smluvních vztazích s partnery tj. smlouvy a související dokumenty např. přílohy. Aplikace bude primárně určená pro evidenci a schvalování smluv s externími partnery. |
|  | Likvidace majetku | Podpora procesu vyřazení a likvidace majetku od vytvoření požadavku přes odeslání oprávněným schvalovatelům, schválení požadavku a potvrzení likvidace. |
|  | Schvalování objednávek | Podpora procesu schvalování objednávek nákupu zboží či služeb včetně schvalování. |
|  | **Funkční požadavky a požadované vlastnosti modulu Smlouvy** | |
|  | Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího datum požadavku, předmět smlouvy, protistranu, způsob financování, lokalitu, finanční objem, způsob schvalování, dotčená oddělení, předkladatele a přílohy. |
|  | Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle vyplnění finančního objemu. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. |
|  | Výstup | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku a jeho schválení (schvalovatelé, data schválení, komentáře). |
|  | **Funkční požadavky a požadované vlastnosti modulu Likvidace majetku** | |
|  | Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího datum požadavku, předmět(y) likvidace (včetně inventárního čísla, popisu, počtu, data pořízení, umístění), lokalitu, dotčená oddělení a střediska, typ likvidace, způsob schvalování, předkladatele a přílohy. |
|  | Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle způsobu likvidace. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. |
|  | Výstup | Po schválení bude automaticky vygenerován PDF soubor a uložen do deníku požadavky, obsahující informace o požadavku stanoviscích schvalovatelů (komise), rozhodnutí a potvrzení o provedení likvidace. |
|  | **Funkční požadavky a požadované vlastnosti modulu Schvalování objednávek** | |
|  | Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, dodavatele, předmět(y), objednávky (včetně popisu, počtu, ceny, dodací lhůty), lokalitu, dotčená oddělení a střediska, žadatele a přílohy. |
|  | Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu ceny. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. |
|  | Výstup | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku a jeho schválení (schvalovatelé, data schválení, komentáře). |
|  | **Společné požadavky** | |
|  | Lokalizace | Lokalizované uživatelské rozhraní |
|  | Zabezpečený přístup | Zabezpečený přístup do aplikace včetně integrovaného přihlašování do uživatelského prostředí i konzol prostřednictvím účtu Active Directory, řízení oprávnění přístupu k informacím. |
|  | Active Directory | Automatické načítání vztahu zaměstnance a jeho nadřízeného. |
|  | Uživatelská přívětivost | Intuitivní grafické rozhraní - prostředí bude odpovídat moderním trendům a zvyklostem - přehlednost, rychlá orientace bez nutnosti čtení textů, využití piktogramů či ikon, kontextové nápovědy. Vhodné pro použití na mobilních (dotykových) zařízeních. |
|  | Integrace | Integrace s HELIOS Green pro získávání potřebných údajů (o majetku dle inventárního čísla) v rozsahu funkcí API HELIOS Green. Automatizace a usnadnění práce uživatelů při vyplňování požadavků, prevence chybných zadání. |
|  | API | Systém umožňuje rozšíření funkcí a ovládání pomocí otevřeného rozhraní API |
|  | Licence | pro 1200 uživatelů pracujících na 750 koncových zařízení (stávající licence zákazníka) |
|  | Vyhledávání | Fulltextové vyhledávání napříč požadavky |
|  | Záruka | 12 měsíců včetně nároku na opravné verze |

* 1. Specifické požadavky K3 – Řízení virtuálních desktopů
     + 1. Systém řízení virtuálních desktopů bude určen pro automatizaci a zrychlení přístupu vybraných uživatelů k jejich aplikacím.
       2. Systém umožní rychlé přihlašování uživatelů k virtuálním desktopům pomocí dvoufaktorového (volitelně vícefaktorového) ověření s využitím běžné bezkontaktní karty (faktory – „něco vlastním“ (např. kartu), „něco vím“ (např. pin). Systém musí umožnit ověřování uživatelů i pomocí běžné zabezpečené karty (Smartkarty) připojením odpovídající čtečky karet. Čtečky ani karty nejsou součástí dodávky.
       3. Systém umožní odhlášení uživatele nebo uzamčení či odpojení jeho relace opětovnou aktivací bezkontaktní karty, popř. deaktivací (vyjmutím) kontaktní karty.
       4. Systém umožní automatizovat spuštění uživatelských aplikací po přihlášení uživatele. Podle přihlášeného uživatele budou automaticky spuštěny předvolené aplikace a uživatel do nich bude automaticky přihlášen bez potřeby interakce uživatele. Uživatel tak pouhým přihlášením k virtuálnímu desktopu získá plně připravené a funkční pracovní prostředí rychle a bez prodlev způsobených ručním přihlašováním do aplikací.
       5. Systém umožní rychlou migraci uživatelů mezi pracovišti (tenkými klienty) – po ukončení práce na jednom pracovišti (tenkém klientu) potvrzeném aktivací karty dostane uživatel k dispozici pracovní prostředí na jiném pracovišti ve stejném stavu, jako jej opustil na předchozím pracovišti okamžitě po přihlášení kartou (bez opětovného spouštění aplikací) a to v řádu jednotek sekund.
       6. Systém je možné implementovat i na fyzické počítače – desktopy.
       7. Systém lze realizovat jako samostatný s integrací (sdílení identit a profilů/politik) se stávajícím systémem pro single-sign-on a vícefaktorové ověřování nebo rozšířením stávajího systému pro single-sign-on a vícefaktorové ověřování.

|  |  |  |
| --- | --- | --- |
| **Komodita K3 - Systém pro řízení virtuálních desktopů** | | |
| **Část** | **Parametr** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** |
| **Ověřovací platforma** | Obecné požadavky | Platforma pro zajištění centrálních (serverových) služeb vícefaktorového a jednotného (SSO - single sing-on) ověřování |
|  | Klientské systémy | Podpora desktopových a serverových Windows OS (verze 7/2008 a vyšší) a Linuxu |
|  | Vysoká dostupnost | Vysoce dostupná architektura z 2 automaticky zastupitelných prvků (cluster apod.) s jednotnou správou celého řešení |
| **Imprivata SSO, AM a VDA pro 1200 uživatelů** | Virtualizace | Podpora provozu ve virtuálním prostředí nabízené serverové virtualizace |
|  | Bezpečnost | Ověřování administrátorských účtů vůči Active Directory |
|  | Adresářové služby | Podpora běžných adresářových služeb - Active Directory, NetWare NDS/eDirectory |
|  | Bezpečná komunikace | Komunikace mezi jednotlivými komponenty řešení (klient, server, adresářová služba) je šifrována (SSL či kompatibilní) |
|  | Licence | pro 1200 uživatelů |
|  | Záruka | Záruka včetně nároku na opravné verze 12 měsíců. |
| **Vícefaktorové ověřování** | Obecné požadavky | Zajištění ověření uživatele pro přihlášení k pracovní stanici (PC nebo tenký klient) s využitím více faktorů |
|  | Ověřovací metody | Podpora autentizačních předmětů (kontaktní čipové karty, bezkontaktní karty, USB a bezkontaktní tokeny), biometrických prvků (otisk prstu), kombinace jméno/heslo (s vazbou i bez vazby na Active Directory), PINu a jejich vzájemných kombinací. |
| **Imprivata SSO, AM a VDA pro 1200 uživatelů** | Dynamické ověřování | Podpora konfigurace podmínek pro využití vícefaktorového ověřování - dvoufaktorové ověřování povinné jen při prvním přihlášení v daném dni (pro další přihlášení postačí jeden faktor) |
|  | Virtualizované aplikace a desktopy | "Bezešvá" integrace přihlašovacího procesu bez nutnosti opakovaně zadávat přihlašovací údaje a potvrzovat připojovací dialogy s nejběžnějšími produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix XenApp/XenDesktop) |
|  | Tencí klienti | Podpora náhrady běžného uživatelského rozhraní tenkého klienta přihlašovací obrazovkou pro vícefaktorové ověřování |
|  | Scénáře | Podporované scénáře použití "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi". Koncovou stanicí může být tenký klient i běžný počítač s OS Windows/Linux. |
|  | Licence | pro 1200 uživatelů |
|  | Záruka | Záruka včetně nároku na opravné verze 12 měsíců. |
| **Jednotné přihlašování** | Obecné požadavky | Podpora jednotného (SSO) automatického přihlášení uživatele do libovolných desktopových aplikací včetně jejich automatického spuštění pro přihlášení do operačního systému. |
|  | Podporované aplikace | Podpora SSO do různých typů aplikací - Win aplikace, webové aplikace včetně Java aplikací, terminálové aplikace používající znakové rozhraní apod. Funkčnost nesmí vyžadovat úpravu aplikací. |
|  | Bezpečnost | Přihlašovací údaje do aplikací bude dostupné jen příslušnému uživateli. Přihlašovací údaje musí být ukládány v ověřovací platformě a být centrálně dostupné na libovolném koncovém zařízení (počítač, tenký klient) v síti. |
| **Imprivata SSO, AM a VDA pro 1200 uživatelů** | Profily | Intuitivní podpora vytváření a správu předpisů (profilů) pro jednotlivé aplikace (bez psaní kódu, používání řádkových příkazů apod.). Vytvořené předpisy (profily) aplikací musí být možné přidělovat uživatelům na základě členství v Active Directory skupinách. |
|  | Licence | pro 1200 uživatelů |
|  | Záruka | Záruka včetně nároku na opravné verze 12 měsíců. |

* 1. Architektura technického řešení
     + 1. Architektura komodit je navržena tak, aby vhodně využívala a doplňovala stávající prostředky.
       2. Architektura komodit K1 a K2 bude implementována jako třívrstvá (prezenční, aplikační a datové vrstva) s tenkým klientem – internetovým prohlížečem.
       3. Aplikační a datovou vrstvu architektury komodity K1 bude možné implementovat jako vysoce dostupnou (redundantní) včetně možnosti rozkládání zátěže na jednotlivé prvky vrstvy. Případné rozšiřující licence nejsou součástí zakázky.
       4. Architektura komodit bude využívat jednotnou společnou datovou základnu (databázový stroj)
  2. Integrace
     + 1. Systémy komodit K1 a K2 budou integrovány se stávajícím systémem Active Directory a podporovat jednotné přihlašování SSO (Single sign on) pro rychlé přihlášení a přístup uživatelů.
  3. Rozhraní
     + 1. Řešení komodity K1 a K2 disponuje dokumentovaným, programovým aplikačním rozhraním – API, které bude součástí dodávky včetně dokumentace.
       2. Veškerá uživatelské rozhraní a rozhraní pro běžnou správu a konfiguraci systémů komodit K1 a K2 budou v českém jazyce.
  4. Kompatibilita s ostatními systémy
     + 1. Veškeré serverové softwarové komponenty nabízených řešení budou provozovány ve virtuálním prostředí serverové virtualizace Hyper-V a jsou pro běh v těchto prostředí výrobcem podporovány.
       2. Veškeré serverové softwarové komponenty komodit K1 a K2 budou z důvodu jednotné správy a zálohování provozovány v prostředí Microsoft Windows Server a jsou pro běh v těchto prostředí výrobcem podporovány. Potřebné licence Windows Server zajistí Zadavatele a nejsou předmětem této zakázky.
  5. Typy klientů
     + 1. Klienti systémů dodaných v rámci předmětu plnění musí být podporováni v prostředí aplikační virtualizace MS RDS (Remote desktop services) a v prostředí operačních systémů Windows 7 a vyšší.
       2. Webová rozhraní nabízených komodity musí být funkční v obvyklých internetových prohlížečích – min. Internet Explorer, Edge, Chrome, Firefox, Safari v aktuálních verzích.
  6. Bezpečnost informací
     + 1. Bezpečnost interní i externí komunikace webových rozhraní řešení všech komodit je možno zajistit použitím šifrování (např. SSL) odpovídajícího protokolu (např. HTTPS)
  7. Dokumentace
     + 1. Součástí komodity K1 bude podrobná příručka v českém jazyce pro uživatele i správce (administrátory) detailně a názorně popisující užívání systému a jeho správu včetně změn konfigurace (vytváření/změna workflow, reporty).
  8. Popis povinných parametrů dodávaného řešení
     + 1. V dále uvedené tabulce tabulkách jsou uvedeny parametry dodávaného řešení.

| **Komodita K1 - Správa identit** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Systém pro správu identity (Identity management - IDM)**  **AC IDENTITA** | Základní funkce | Systém pro správu identit - Identity management (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi. | Systém pro správu identit - Identity management (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Licence | Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Minimální počet spravovaných uživatelů je 2100. | Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Počet spravovaných uživatelů je 2100. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Škálovatelnost | Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. | Systém umožňuje zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Evidence aplikací a rolí | Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby. | Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Uživatelské role | Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS. | Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Historizace | Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti. | Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Automatizace | Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). | Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Logování SIEM | Systém bude poskytovat auditní logy ve formátu vhodném pro systém typu SIEM (Security Information and Event Management) | Systém poskytuje auditní logy ve formátu vhodném pro systém typu SIEM (Security Information and Event Management) | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Logování systému | Systém obsahuje logování min. následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log) | Systém obsahuje logování následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log) | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Správa identit | Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury. | Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Systematizovaná místa | Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu. | Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Podpora eIDAS | Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. | Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Vysoká dostupnost | Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti. | Systém je možno nasadit na více serverů v režimu vysoké dostupnosti. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Požadavky na portál - obecné | IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. | IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Podpora mobilních zařízení | Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno) | Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno) | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Správa referenčních objektů | Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát. | Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Referenční objekty | Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity | Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Zabezpečení referenčních objektů | Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů | Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Rozšiřující atributy | Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM. | Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Přehledné zobrazení | Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit). | Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit). | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Vyhledávání - diakritika | Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.) | Portál bude umožňovat vyhledávat i bez diakritiky (zadání Parizek vyhledává i Pařízek apod.) | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Správa certifikátů | Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti. | Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Obrázky | Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie. | Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Přesun identit | Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními. | Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Kopírování rolí | Systém umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy. | Systém umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Ochrana proti chybám | Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod). | Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod). | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Aktivní uživatelé | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Slučování identit | Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů. | Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Export údajů | Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu | Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Filtrování | Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití. | Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Správa oprávnění | Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) | Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Granularita oprávnění | Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět. | Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Oprávnění k atributům | Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů. | Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Kontextový výběr | Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky. | Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Správa licencí | IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow. | IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Časová omezení | IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere. | IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Vícenásobné vazby | Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. | Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Přehled rolí | Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role. | Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Přehled dědičností | IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu. | IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Skupiny | IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. | IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Zastupitelnost | IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta,…) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce. | IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Delegování oprávnění | Možnost delegování administrátorských práv. | Možnost delegování administrátorských práv. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Správa osobních údajů | IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací. | IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Osobní údaje | IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům. | IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Osobní údaje - automatizace | IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů. | IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Obnovení hesla | IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu). | IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. IDM je možné na SMS bránu či službu napojit). Rozhraní bude umožňovat i běžnou změnu hesla (bez resetu). | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Žádosti | IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení. | IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Externí subjekty | IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin. | IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Kontextový výběr | Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat. | Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Individualizace | IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně. | IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Workflow | Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele  - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění  - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů | Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele  - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění  - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Workflow - sledování | Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude ve obvyklém formátu pro zobrazní workflow např. aktivity diagram, BPMN nebo Archimate | Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazní workflow aktivity diagram, BPMN nebo Archimate | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Upozornění | IDM zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. | IDM zajistí zasílání konfigurovatelných emailových upozornění pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Včasná upozornění | Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně. | Upozornění na vypršení časových termínů bude možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Šablony upozornění | Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu. | Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám bude možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony bude umožňovat vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Kontext upozornění | Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd. | Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Logování | Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu. | Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Důvěryhodnost logování | Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM. | Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Provozní stav | Kumulovaný online přehled o aktuálním stavu hlavních částí systému a případných chybách - min. chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu workflow. | Kumulovaný online přehled o aktuálním stavu hlavních částí systému a případných chybách - min. chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu workflow. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Auditní report | IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. | IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Auditní report - výběr | Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů. | Identity pro generování auditního reporty bude možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Reporty uživatelů | Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru. | Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Reporty - zasílání | Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel. | Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Reporty - historie | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Reporty - porovnání | Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu. | Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Webové služby (WS) | IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. | IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Standardy WS | Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. | Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Bezpečnost WS | Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. | Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Logování WS | Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu | Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Služby rozhraní WS | Rozhraní bude poskytovat minimálně následující služby: - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu funkcí / rolí  - Získání seznamu uživatelů dané aplikace - Získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci - Zápis seznamu funkcí do IDM - Zápis certifikátů do IDM - Zápis a změna identit | Rozhraní bude poskytovat minimálně následující služby: - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu funkcí / rolí  - Získání seznamu uživatelů dané aplikace - Získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci - Zápis seznamu funkcí do IDM - Zápis certifikátů do IDM - Zápis a změna identit | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Synchronizace | Ruční i automatické spuštění synchronizací s propojenými systémy. | Ruční i automatické spuštění synchronizací s propojenými systémy. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Synchronizace - simulace | Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu. | Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Simulace - průběh | Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě. | Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Synchronizace - režimy | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému):  - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému  - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace.  - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.  - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému.  - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka.  - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala. | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému):  - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému  - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace.  - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.  - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému.  - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka.  - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Synchronizace - správa | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu. | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Obecné konektory | Vestavěné obecné konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL - konektor pro napojení na SOAP a REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3 | Vestavěné obecné konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL - konektor pro napojení na SOAP a REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3 | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Speciální konektory | IDM bude obsahovat konektor umožňující správu virtuálních aplikací. Požadavky na správu identit ve virtuálních aplikacích bude IDM předávat e-mailem správcům odpovídajících reálných aplikací. Správci potvrdí splnění požadavku zpět do IDM. Uvedeným systémem budou řízeny identity v aplikacích, které nelze nebo není ekonomicky efektivní integrovat s IDM pomocí obecných nebo aplikačních konektorů. | IDM bude obsahovat konektor umožňující správu virtuálních aplikací. Požadavky na správu identit ve virtuálních aplikacích bude IDM předávat e-mailem správcům odpovídajících reálných aplikací. Správci potvrdí splnění požadavku zpět do IDM. Uvedeným systémem budou řízeny identity v aplikacích, které nelze nebo není ekonomicky efektivní integrovat s IDM pomocí obecných nebo aplikačních konektorů. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Aplikační konektory | IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet a spravovat uživatelské účty a jejich oprávnění včetně souvisejících operací potřebných pro plnou automatizaci správy identit v daném systému (např. řízení členství ve skupinách, přiřazení rolí, správa metadat): - Microsoft Active Directory - ekonomický systém Helios Green (Asseco) - NIS tj. nemocniční informační systém) Fons Enterprise (Stapro) - Laboratorní systém OpenLims (Stapro) - PACS - MARIE PACS (OR-CZ) - groupware IceWarp Mail Server, včetně vytváření schránek (IceWarp)  - docházkový systém (IVAR) - Service desk (Alvao) - Asset management (Alvao) - DMS - Komodita K2 | IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet a spravovat uživatelské účty a jejich oprávnění včetně souvisejících operací potřebných pro plnou automatizaci správy identit v daném systému (řízení členství ve skupinách, přiřazení rolí, správa metadat): - Microsoft Active Directory - ekonomický systém Helios Green (Asseco) - NIS tj. nemocniční informační systém) Fons Enterprise (Stapro) - Laboratorní systém OpenLims (Stapro) - PACS - MARIE PACS (OR-CZ) - groupware IceWarp Mail Server, včetně vytváření schránek (IceWarp)  - docházkový systém (IVAR) - Service desk (Alvao) - Asset management (Alvao) - DMS - Komodita K2 | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Zdrojový systém | IDM bude napojeno na personální systém Avensio (Alfa software). Z personálního systému budou načítány údaje o organizační struktuře, pracovních místech a funkcích, osobách a tyto údaje budou pro IDM sloužit jako zdrojové | IDM bude napojeno na personální systém Avensio (Alfa software). Z personálního systému budou načítány údaje o organizační struktuře, pracovních místech a funkcích, osobách a tyto údaje budou pro IDM sloužit jako zdrojové | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Záruka | Min. 12 měsíců včetně nároku na opravné verze | 12 měsíců včetně nároku na opravné verze | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |

| **Komodita K2 - Správa provozních dokumentů** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Systém pro správu dokumentů**  **Funkční rozšíření stávajícího řešení ALVAO** | Základní funkce | DMS systém (Document management systém - dále jen DMS nebo systém) - systém koncipovaný jako portál dostupný prostřednictvím webového prohlížeče, obsahující dále uvedené aplikace či moduly a funkce. | DMS systém (Document management systém - dále jen DMS nebo systém) - systém koncipovaný jako portál dostupný prostřednictvím webového prohlížeče, obsahující dále uvedené aplikace či moduly a funkce. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| **Aplikace - moduly** | | | |
| Smlouvy | Obsahuje podklady o smluvních vztazích s partnery tj. smlouvy a související dokumenty např. přílohy. Aplikace bude primárně určená pro evidenci a schvalování smluv s externími partnery. | Obsahuje podklady o smluvních vztazích s partnery tj. smlouvy a související dokumenty např. přílohy. Aplikace bude primárně určená pro evidenci a schvalování smluv s externími partnery. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Likvidace majetku | Podpora procesu vyřazení a likvidace majetku od vytvoření požadavku přes odeslání oprávněným schvalovatelům, schválení požadavku a potvrzení likvidace. | Podpora procesu vyřazení a likvidace majetku od vytvoření požadavku přes odeslání oprávněným schvalovatelům, schválení požadavku a potvrzení likvidace. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Schvalování objednávek | Podpora procesu schvalování objednávek nákupu zboží či služeb včetně schvalování. | Podpora procesu schvalování objednávek nákupu zboží či služeb včetně schvalování. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| **Funkční požadavky a požadované vlastnosti modulu Smlouvy** | | | |
| Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, předmět smlouvy, protistranu, způsob financování, lokalitu, finanční objem, způsob schvalování, dotčená oddělení, předkladatele a přílohy. | Prostřednictvím upravitelného formuláře obsahujícího datum požadavku, předmět smlouvy, protistranu, způsob financování, lokalitu, finanční objem, způsob schvalování, dotčená oddělení, předkladatele a přílohy. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle vyplnění finančního objemu. Min. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle vyplnění finančního objemu. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Výstup | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku (v rozsahu viz. Vytvoření požadavku) a jeho schválení (schvalovatelé, data schválení, komentáře). | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku a jeho schválení (schvalovatelé, data schválení, komentáře). | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| **Funkční požadavky a požadované vlastnosti modulu Likvidace majetku** | | | |
| Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, předmět(y) likvidace (včetně inventárního čísla, popisu, počtu, data pořízení, umístění apod.), lokalitu, dotčená oddělení a střediska, typ likvidace, způsob schvalování, předkladatele a přílohy. | Prostřednictvím upravitelného formuláře obsahujícího datum požadavku, předmět(y) likvidace (včetně inventárního čísla, popisu, počtu, data pořízení, umístění), lokalitu, dotčená oddělení a střediska, typ likvidace, způsob schvalování, předkladatele a přílohy. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle způsobu likvidace. Min. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle způsobu likvidace. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Výstup | Po schválení bude automaticky vygenerován PDF soubor a uložen do deníku požadavky, obsahující informace o požadavku (v rozsahu viz. Vytvoření požadavku), stanoviscích schvalovatelů (komise), rozhodnutí a potvrzení o provedení likvidace. | Po schválení bude automaticky vygenerován PDF soubor a uložen do deníku požadavky, obsahující informace o požadavku stanoviscích schvalovatelů (komise), rozhodnutí a potvrzení o provedení likvidace. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| **Funkční požadavky a požadované vlastnosti modulu Schvalování objednávek** | | | |
| Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, dodavatele, předmět(y) objednávky (včetně popisu, počtu, ceny, dodací lhůty), lokalitu, dotčená oddělení a střediska, žadatele a přílohy. | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, dodavatele, předmět(y), objednávky (včetně popisu, počtu, ceny, dodací lhůty), lokalitu, dotčená oddělení a střediska, žadatele a přílohy. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu ceny. Min. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu ceny. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Výstup | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku (v rozsahu viz. Vytvoření požadavku) a jeho schválení (schvalovatelé, data schválení, komentáře). | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku a jeho schválení (schvalovatelé, data schválení, komentáře). | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| **Společné požadavky** | | | |
| Lokalizace | Lokalizované uživatelské rozhraní | Lokalizované uživatelské rozhraní | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Zabezpečený přístup | Zabezpečený přístup do aplikace včetně integrovaného přihlašování do uživatelského prostředí i konzol prostřednictvím účtu Active Directory, řízení oprávnění přístupu k informacím. | Zabezpečený přístup do aplikace včetně integrovaného přihlašování do uživatelského prostředí i konzol prostřednictvím účtu Active Directory, řízení oprávnění přístupu k informacím. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Active Directory | Automatické načítání vztahu zaměstnance a jeho nadřízeného. | Automatické načítání vztahu zaměstnance a jeho nadřízeného. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Uživatelská přívětivost | Intuitivní grafické rozhraní - prostředí bude odpovídat moderním trendům a zvyklostem - přehlednost, rychlá orientace bez nutnosti čtení textů, využití piktogramů či ikon, kontextové nápovědy. Vhodné pro použití na mobilních (dotykových) zařízeních. | Intuitivní grafické rozhraní - prostředí bude odpovídat moderním trendům a zvyklostem - přehlednost, rychlá orientace bez nutnosti čtení textů, využití piktogramů či ikon, kontextové nápovědy. Vhodné pro použití na mobilních (dotykových) zařízeních. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Integrace | Integrace s HELIOS Green pro získávání potřebných údajů (např. o majetku dle inventárního čísla) v rozsahu funkcí API HELIOS Green. Automatizace a usnadnění práce uživatelů při vyplňování požadavků, prevence chybných zadání. | Integrace s HELIOS Green pro získávání potřebných údajů (o majetku dle inventárního čísla) v rozsahu funkcí API HELIOS Green. Automatizace a usnadnění práce uživatelů při vyplňování požadavků, prevence chybných zadání. | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| API | Systém musí umožnit rozšíření funkcí a ovládání pomocí otevřeného rozhraní API | Systém umožňuje rozšíření funkcí a ovládání pomocí otevřeného rozhraní API | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Licence | Min. pro 1200 uživatelů pracujících na 750 koncových zařízení. | pro 1200 uživatelů pracujících na 750 koncových zařízení (stávající licence zákazníka) | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Vyhledávání | Fulltextové vyhledávání napříč požadavky | Fulltextové vyhledávání napříč požadavky | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |
| Záruka | Min.12 měsíců včetně nároku na opravné verze | 12 měsíců včetně nároku na opravné verze | 8.3 Specifické požadavky K2 – Správa provozních dokumentů |

| **Komodita K3 - Systém pro řízení virtuálních desktopů** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Ověřovací platforma**  **Imprivata SSO, AM a VDA pro 1200 uživatelů** | Obecné požadavky | Platforma pro zajištění centrálních (serverových) služeb vícefaktorového a jednotného (SSO - single sing-on) ověřování | Platforma pro zajištění centrálních (serverových) služeb vícefaktorového a jednotného (SSO - single sing-on) ověřování | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Klientské systémy | Podpora desktopových a serverových Windows OS (verze 7/2008 a vyšší) a Linuxu | Podpora desktopových a serverových Windows OS (verze 7/2008 a vyšší) a Linuxu | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Vysoká dostupnost | Vysoce dostupná architektura z minimálně 2 automaticky zastupitelných prvků (cluster apod.) s jednotnou správou celého řešení | Vysoce dostupná architektura z 2 automaticky zastupitelných prvků (cluster apod.) s jednotnou správou celého řešení | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Virtualizace | Podpora provozu ve virtuálním prostředí nabízené serverové virtualizace | Podpora provozu ve virtuálním prostředí nabízené serverové virtualizace | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Bezpečnost | Ověřování administrátorských účtů vůči Active Directory | Ověřování administrátorských účtů vůči Active Directory | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Adresářové služby | Podpora běžných adresářových služeb - Active Directory, NetWare NDS/eDirectory | Podpora běžných adresářových služeb - Active Directory, NetWare NDS/eDirectory | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Bezpečná komunikace | Komunikace mezi jednotlivými komponenty řešení (klient, server, adresářová služba apod.) je šifrována (SSL či kompatibilní) | Komunikace mezi jednotlivými komponenty řešení (klient, server, adresářová služba) je šifrována (SSL či kompatibilní) | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Licence | Min. pro 1200 uživatelů | pro 1200 uživatelů | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Záruka | Záruka včetně nároku na opravné verze min. 12 měsíců. | Záruka včetně nároku na opravné verze 12 měsíců. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| **Vícefaktorové ověřování**  **Imprivata SSO, AM a VDA pro 1200 uživatelů** | Obecné požadavky | Zajištění ověření uživatele pro přihlášení k pracovní stanici (PC nebo tenký klient) s využitím více faktorů | Zajištění ověření uživatele pro přihlášení k pracovní stanici (PC nebo tenký klient) s využitím více faktorů | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Ověřovací metody | Podpora autentizačních předmětů (kontaktní čipové karty, bezkontaktní karty, USB a bezkontaktní tokeny), biometrických prvků (otisk prstu), kombinace jméno/heslo (s vazbou i bez vazby na Active Directory), PINu a jejich vzájemných kombinací. | Podpora autentizačních předmětů (kontaktní čipové karty, bezkontaktní karty, USB a bezkontaktní tokeny), biometrických prvků (otisk prstu), kombinace jméno/heslo (s vazbou i bez vazby na Active Directory), PINu a jejich vzájemných kombinací. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Dynamické ověřování | Podpora konfigurace podmínek pro využití vícefaktorového ověřování - např. dvoufaktorové ověřování povinné jen při prvním přihlášení v daném dni (pro další přihlášení postačí jeden faktor) apod. | Podpora konfigurace podmínek pro využití vícefaktorového ověřování - dvoufaktorové ověřování povinné jen při prvním přihlášení v daném dni (pro další přihlášení postačí jeden faktor) | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Virtualizované aplikace a desktopy | "Bezešvá" integrace přihlašovacího procesu bez nutnosti opakovaně zadávat přihlašovací údaje a potvrzovat připojovací dialogy s nejběžnějšími produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix XenApp/XenDesktop) | "Bezešvá" integrace přihlašovacího procesu bez nutnosti opakovaně zadávat přihlašovací údaje a potvrzovat připojovací dialogy s nejběžnějšími produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix XenApp/XenDesktop) | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Tencí klienti | Podpora náhrady běžného uživatelského rozhraní tenkého klienta přihlašovací obrazovkou pro vícefaktorové ověřování | Podpora náhrady běžného uživatelského rozhraní tenkého klienta přihlašovací obrazovkou pro vícefaktorové ověřování | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Scénáře | Podporované scénáře použití "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi". Koncovou stanicí může být tenký klient i běžný počítač s OS Windows/Linux. | Podporované scénáře použití "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi". Koncovou stanicí může být tenký klient i běžný počítač s OS Windows/Linux. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Licence | Min. pro 1200 uživatelů | pro 1200 uživatelů | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Záruka | Záruka včetně nároku na opravné verze min. 12 měsíců. | Záruka včetně nároku na opravné verze 12 měsíců. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| **Jednotné přihlašování**  **Imprivata SSO, AM a VDA pro 1200 uživatelů** | Obecné požadavky | Podpora jednotného (SSO) automatického přihlášení uživatele do libovolných desktopových aplikací včetně jejich automatického spuštění pro přihlášení do operačního systému. | Podpora jednotného (SSO) automatického přihlášení uživatele do libovolných desktopových aplikací včetně jejich automatického spuštění pro přihlášení do operačního systému. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Podporované aplikace | Podpora SSO do různých typů aplikací - Win aplikace, webové aplikace včetně Java aplikací, terminálové aplikace používající znakové rozhraní apod. Funkčnost nesmí vyžadovat úpravu aplikací. | Podpora SSO do různých typů aplikací - Win aplikace, webové aplikace včetně Java aplikací, terminálové aplikace používající znakové rozhraní apod. Funkčnost nesmí vyžadovat úpravu aplikací. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Bezpečnost | Přihlašovací údaje do aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje musí být ukládány v ověřovací platformě a být centrálně dostupné na libovolném koncovém zařízení (počítač, tenký klient) v síti. | Přihlašovací údaje do aplikací bude dostupné jen příslušnému uživateli. Přihlašovací údaje musí být ukládány v ověřovací platformě a být centrálně dostupné na libovolném koncovém zařízení (počítač, tenký klient) v síti. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Profily | Intuitivní podpora vytváření a správu předpisů (profilů) pro jednotlivé aplikace (bez psaní kódu, používání řádkových příkazů apod.). Vytvořené předpisy (profily) aplikací musí být možné přidělovat uživatelům na základě členství v Active Directory skupinách. | Intuitivní podpora vytváření a správu předpisů (profilů) pro jednotlivé aplikace (bez psaní kódu, používání řádkových příkazů apod.). Vytvořené předpisy (profily) aplikací musí být možné přidělovat uživatelům na základě členství v Active Directory skupinách. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Licence | Min. pro 1200 uživatelů | pro 1200 uživatelů | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |
| Záruka | Záruka včetně nároku na opravné verze min. 12 měsíců. | Záruka včetně nároku na opravné verze 12 měsíců. | 8.4 Specifické požadavky K3 – Řízení virtuálních desktopů |

* 1. Hodnocené parametry technického řešení
     1. Vlastnosti technického řešení
        1. funkční vlastnosti nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **Hodnocené parametry** | | | |
| **Parametr** | **Popis** | **Uchazeč popíše způsob naplnění tohoto hodnoceného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Snížení nároků na správu systému** | | | |
| 1 | Z důvodu zachování jednotné datové základny, její správy a zálohování budou systémy komodit K1 a K2 využívat pro ukládání dat databázový server MS SQL server | Systémy komodit K1 a K2 budou využívat pro ukládání dat databázový server MS SQL server | 9.7 Podklady pro hodnocení |
| **Uživatelské přívětivost a snížení nároků na správu** | | | |
| 2 | Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K1 bude v českém jazyce | Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K1 bude v českém jazyce | 9.7 Podklady pro hodnocení |
| **Integrace s MS Outlook - Komodita K2** | | | |
| 3 | Systém bude integrován s MS Outlook (2010 a vyšší). Integrací se rozumí rozšíření prvků MS Outlook (ribbon – pás karet, formuláře a jejich ovládací prvky) o možnost správy požadavků přímo v prostředí MS Outlook. | Systém Alvao ServiceDesk je plně integrován s prostředím Microsoft Outlouk pomocí speciálního pluginu, který rozšiřuje ovládací prvky MS Outlook o možnost plné správy požadavků – viz. https://www.alvao.cz/produkty/service-desk/ - „Pracujte přímo z Outlooku“ | 9.7 Podklady pro hodnocení |

* 1. Implementační služby
     1. Obecné požadavky
        1. V rámci implementace předmětu plnění Uchazeč realizuje následující služby:
           1. Zajištění projektového vedení realizace předmětu plnění.
           2. Provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Výstupem bude prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Prováděcí dokumentace bude připravena před zahájením realizace dodávek, tzn. po provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu a musí být výslovně schválena Zadavatelem.
           3. Dodávka a implementace nabízených předmětu plnění splňující povinné parametry technického řešení a zajištění technické podpory.
           4. Zpracování provozní dokumentace implementovaného systému v rozsahu popisu implementovaných funkcionalit a popisu činností běžné údržby a administrace systémů. Dokumentace může být poskytnuta i formou lokalizované (české) vestavěné nebo online nápověda či příručky.
           5. Provedení školení,
           6. Zajištění zkušebního provozu,
           7. Provedení akceptačních testů,
           8. Předání do ostrého provozu,
        2. Činnost omezující práci uživatelů budou prováděny mimo běžnou pracovní KKN, tj. mimo pracovní dny 7:00–15:30 hod.

Další specifické služby:

|  |
| --- |
| K1: Správa identit |
| * 1. Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu:      1. analýzu procesů a aplikací KKN se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí,      2. analýzu požadavků KKN zasílaných informačním systémům s požadavkem na autorizaci a autentizaci,      3. technologický popis stávajících technologií s vazbou na systém správy identit      4. analýzu možností správy výstupních struktur,      5. analýzu evidenčních údajů a logů,      6. návrh životního cyklu identity uživatelů,      7. model organizační struktury,      8. seznam systemizovaných pracovních pozic,      9. přiřazení pracovníků k pracovním pozicím,      10. atributy poskytované personálním systémem v souladu s potřebami obsluhovaných systémů a návrh jejich využití,      11. manažerský souhrn vhodný pro prezentaci výstupů analýzy vedení KKN.   2. Návrh a realizace konfiguračních změn infrastruktury   3. Návrh a provedení akceptačních testů, bude zahrnovat výkonové testy a prokázat plnou funkčnost integrací v obvyklých scénářích použití. |

| K2: Správa provozních dokumentů |
| --- |
| * 1. Analýza dokumentů a procesů relevantních pro implementaci požadovaných aplikací - modulů   2. Návrh vhodných datových struktur, kategorií a metadat, přístupových oprávnění a rolí včetně skupin,   3. Návrh a realizace vstupních, stavových a výstupnách formulářů a dokumentů požadavků   4. Analýza funkcionalit API HELIOS Green a realizace potřebných datových importů a/nebo dotazů.   5. Návrh vhodných pracovních postupů (workflow).   6. Implementace systému dle provedených návrhů a doporučení výrobce   7. Návrh a realizace konfiguračních změn infrastruktury   8. Návrh a provedení akceptačních testů |

| K3: Systém pro řízení virtuálních desktopů |
| --- |
| * 1. Návrh systému pro vícefaktorové ověřování uživatelů včetně vhodných politik   2. Návrh začlenění vícefaktorového ověřování uživatelů do prostředí aplikační virtualizace – k dispozici bude vícefaktorové i běžné (jméno, heslo) ověřování   3. Návrh vhodných aplikačních sad pro vybrané uživatelské role a způsob jejich spuštění a automatického přihlašování   4. Návrh způsobu realizace požadovaných scénářů "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi"   5. Implementace systému dle provedených návrhů a doporučení výrobce   6. Návrh a provedení akceptačních testů |

* + 1. Zpracování prováděcí dokumentace
       1. Před zahájením implementačních prací bude zpracována prováděcí dokumentace, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.
       2. Jako podklad pro zpracování prováděcí dokumentace bude zpracována předimplementační analýza, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění uchazeče, zejména pak s ohledem na uchazečem použité technické řešení, pro následující oblasti:
          1. Stávající stav (vstupy) relevantní pro návrh implementace komodity.
          2. Způsob začlenění nabízených komodit do stávajícího prostředí.
          3. Konfigurační změny nabízeného systému potřebné pro naplnění povinných požadavků.
          4. Virtualizační infrastruktura (serverová, síťová, disková i aplikační) ve vztahu k plánovanému využití.
          5. Integrace nabízených softwarových systémů.
          6. Požadované součinnosti Zadavatele a jejich rozsah.
          7. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.
       3. Prováděcí dokumentace zohlední podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného uchazečem a budeí obsahovat tyto části:
          1. Popis cílového stavu / konfigurace nabízeného systému,
          2. Detailní harmonogram realizace včetně uvedení kritických milníků,
          3. Vazby na integrované systémy systémy,
          4. Návrh akceptačních kritérií a akceptačních testů.
       4. Prováděcí dokumentace bude před zahájením realizace dalších etap plnění výslovně schválena zadavatelem.
    2. Harmonogram realizace
       1. Bude zajištěno projektové vedení po celou dobu realizace zakázky projektovým manažerem. Součástí nabídky je metodiky, která bude pro projektové řízení použita.
       2. Harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo. Čísla značí počet kalendářních dnů.

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Etapa projektu – činnost** | **Zahájení etapy** | **Ukončení etapy** |
| 1 | Předimplementační analýza a zhotovení Prováděcí dokumentace včetně vypořádání připomínek a akceptace Zadavatelem | D | D+40 |
| 2 | Dodávky a implementace | D+40 | D+100 |
| 3 | Školení administrátorů | D+80 | D+110 |
| 4 | Zkušební provoz | D+90 | D+100 |
| 5 | Akceptační testy | D+100 | D+110 |
| 6 | Zahájení plného provozu | D+110 | - |

* + 1. Školení
       1. Uchazeč zajistí školení pracovníků Zadavatele – administrátorů– na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to v rozsahu předávané provozní dokumentace ICT a uživatelských příruček k jednotlivým komoditám.
       2. Školení zajistí seznámení administrátorů Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.

Rozsah školení pro administrátory je:

* + - * 1. 8 hodin pro komoditu K1
        2. 4 hodiny pro komoditu K2
        3. 4 hodiny pro komoditu K3
      1. Školení bude probíhat v sídle Zadavatele.
      2. Předpokládá se účast max. 5 administrátorů.
    1. Provedení akceptačních testů, zkušební provoz a přechod do ostrého provozu
       1. Součástí akceptačních testů bude pro každou komoditu:
          1. Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.
          2. Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.
          3. Prokázání přiměřených odezev systému při náročnějších operacích
          4. Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
       2. Pro každou komoditu budou navrženy vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení.
       3. O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
       4. Uchazeč zajistí zkušební provozu v délce 10 dnů včetně technické podpory 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
       5. Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.
  1. Záruky a servisní podmínky
     + 1. Záruka na veškeré dodané služby v délce trvání 3 měsíců a zařízení 24 měsíců (není-li u konkrétní komodity uvedeno jinak) od okamžiku ukončení implementace a předání do produkčního provozu.
       2. Není-li u konkrétní komodity uvedeno jinak, bude provedení záruční opravy do 5-ti pracovních dnů nebo poskytnutí náhradního prvku shodných nebo lepších parametrů po dobu opravy.
       3. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.
       4. Bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit po dobu záruky.
       5. Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro Zadavatele.
       6. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
       7. Pro hlášení servisní požadavků zajistí Uchazeč Zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy je součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 7-17 hod. v pracovních dnech.
  2. Zabezpečení provozu

### Definice

* + - 1. **24x7** – služba nebo zařízení je v provozu/dostupné 24 hodin a 7 dní v týdnu s garancí minimálně 95% dostupnosti
      2. **9x5** - služba nebo zařízení je v provozu/dostupné 9 hodin denně v běžnou pracovní dobu po všechny pracovní dni v týdnu s garancí minimálně 95% dostupnosti
      3. **BD** – Business Day – standartní pracovní den
      4. **BE (Best Effort)** - Uchazeč vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů Prvku IT v nejkratší možné době.
      5. **Bezpečnostní incident -** stav nebo událost, která je v rozporu interní směrnicí Zadavatele související s provozem ICT nebo událost, která způsobila nehodu nebo potenciálně mohla způsobit omezení případně nefunkčnost ICT. Zahrnuje též kybernetické bezpečnostní incidenty - kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
      6. **Běžná pracovní doba** – čas mezi 8:00 a 17:00 v Pracovní dny.
      7. **Člověkohodina** - práce pracovníka Uchazeče v rozsahu jedné (1) hodiny v rámci Pracovního dne.
      8. **Člověkoden** - práce pracovníka Uchazeče v rozsahu jednoho (1) Pracovního dne.
      9. **Doba odezvy (Response time – R)** – metrika definující čas, který uplyne od nahlášení Požadavku na Servisní službu do začátku provádění Servisní služby. Do Doby odezvy se započítává pouze čas, určený Servisním kalendářem k řešení daného Požadavku. Za odezvu se považuje jakákoliv prokazatelná reakce servisního pracovníka Uchazeč směřující k odstranění Incidentu, zodpovězení Dotazu nebo přípravy Nového požadavku.
      10. **Dotaz** – funkce v systému existuje, Prvek IT pracuje v souladu s Prováděcí dokumentací, ale pověřená osoba zákazníka s ní není dostatečně seznámena a podá Požadavek - Dotaz na Hot-line nebo HelpDesk
      11. **HelpDesk** – nepřetržitě dostupný automatizovaný systém pro vzdálené zadávání a správu požadavků,
      12. **Hot-line** –pracoviště Uchazeče přijímající Požadavky od Zadavatele na definovaných telefonních číslech nebo elektronických komunikačních kanálech.
      13. **Odborná podpora** – konzultace, technická pomoc
      14. **Incident**- událost způsobující odchylku od očekávané funkce Prvku IT, která způsobuje nebo může způsobit přerušení anebo snížení kvality této funkce.
      15. **Priorita Incidentu** - závažnost Incidentu dle klasifikace Kontaktní osoby Zadavatele.
      16. **Koncová zařízení** - počítače uživatelů, jejich základní programové vybavení a periferní zařízení k počítačům připojená (např. tiskárny, skenery).
      17. **Monitorování –** jedná se o službu nepřetržitého online monitorování systémů s upozorněním na kritické nebo neobvyklé události a provozní hodnoty Prvků IT, upozornění budou automaticky zasílána oprávněným pracovníkům Zadavatele. Součástí služby je vzdálený přístup k aktuálním i historickým údajům o stavu systému.
      18. **Proaktivní monitorování** - monitorování prováděné dle charakteru provozu a činnosti Prvků IT v režimu 9x5. Při zjištění Incidentu je monitorovacím systém a/nebo manuálně pracovníkem Uchazeče založen Požadavek a zahájeno jeho řešení podle kategorie Incidentu
      19. **Náhradní zařízení** – zařízení podobných vlastností (parametrů).
      20. **Požadavek** - žádost o provedení Servisní služby na jednom nebo více Prvcích IT.

Požadavek může zahrnovat:

* + - * 1. žádost o odstranění závady (nefunkční Prvek IT nebo nesprávná činnost Prvku IT) - Incidentu
        2. žádost o poskytnutí konzultace
        3. žádost o provedení Změny

Požadavek může:

* + - * 1. být zadán Zadavatelem jako jednorázový
        2. být zadán Zadavatelem jako opakující se činnost
        3. vzniknout jako výstup Monitorování
        4. vzniknout na základě Správy a údržby Prvku IT
      1. **NBD**-**Next Business Day** – následující pracovní den
      2. **Neprodleně** – bez zbytečného odkladu, s vyvinutím maximálního úsilí na zjednání nápravy nebo zajištění činnosti, nejpozději však následující Pracovní den.
      3. **Pracovní dny** - všechny dny, kromě sobot a nedělí nebo zákonem stanovených svátků a dnů pracovního klidu, během nichž dohodnuté pracovní činnosti budou prováděny v čase od 8:00 do 17:00 hodin.
      4. **Prvek IT** - zařízení (Koncové zařízení, server či jiný hardware), program (software) nebo komunikační linka.
      5. **Rozsah poskytovaných služeb** – specifikace Služby a kvantifikace rozsahu Služby
      6. **Řešitel** - pracovník Uchazeče, podílející se na řešení Požadavku.
      7. **Report** – přehledový dokument, ve kterém je popsán průběh realizace Plnění za uplynulé období a hodnoty sledovaných parametrů.
      8. **SLA (Service Level Agreement)** - definice kvalitativních parametrů/metrik Služby
      9. **Správa a údržba** - provádění činností, které jsou nutné ke správné a bezchybné funkci Prvku IT. Zpravidla se jedná o pravidelnou kontrolu stavu Prvků IT a provádění takových Změn, které se pravidelně opakují, nebo jsou provedeny na základě kontroly stavu Prvku IT.
      10. **Služby** – činnosti potřebné pro řádné zabezpečení podpory provozu předmětu plnění.
      11. **Úplné odstranění závady** - se rozumí dosažení stavu, který byl akceptován v rámci smlouvy o dílo nebo je popsán v prováděcí dokumentaci popř. v dokumentaci Prvku IT.
      12. **Vzdálená správa** – provádění činností na Prvcích IT, přičemž činnosti nejsou prováděny v místě provozovny Zadavatele, ale prostřednictvím Vzdáleného přístupu z místa provozovny Uchazeče.
      13. **Vzdálený přístup** – připojení z provozovny Uchazeče k zařízení Zadavatele pomocí komunikační linky, na které je vytvořeno dočasné nebo trvalé spojení.
      14. **Zprovoznění náhradním způsobem** - se rozumí zajištění základních funkcí systému, tedy dosažení stavu, kdy není vážně omezena funkčnost informačního systému nebo jeho částí.
      15. **Změna** - změna parametrů Prvku IT nebo instalace, přemístění či odinstalace Prvku IT.
      16. **Legislativní servis -** legislativním servisem se rozumí úprava stávající funkčnosti stávajícího systému (software), kterou je nutné provést, protože stávající funkcionalita by nutila zákazníka konat v rozporu s novou legislativní úpravou. Legislativní úpravou v žádném případě není doplnění funkcionality (řešené oblasti), kterou stávající systém (software) nepokrýval.
      17. **Reklamace -** reklamací je požadavek vznesený na přezkoumání a odstranění vlastnosti Prvku IT v čase záruční doby, která je v rozporu:
          1. se standardní funkčností Prvku IT a tento rozpor je vůči uživatelské dokumentaci produktu,
          2. s funkcionalitou definovanou ve smlouvě (jejích přílohách), případně akceptačním protokolu funkcionality Prvku IT,
          3. s platnou legislativou ČR k datu podání požadavku.
      18. **Konfigurační management** - jde o službu poskytovanou za účelem udržení aktuální technické dokumentace. V případě jakékoliv provedené změny, bude aktualizována provozní dokumentace ICT o konfiguraci systému včetně zaznamenaných změn. Dokumentace bude uložena u Uchazeče i Zadavatele. Poskytuje informace o Prvcích IT a službách včetně informací o aktuálních verzích. Zahrnuje rovněž správu veškeré dokumentace ke všem prvkům infrastruktury a služeb. Obvykle je využíván automatizovaný nástroj pro sběr a aktualizaci většiny údajů v konfigurační databázi.
      19. **Patch Management -** jedná se o preventivní činnost týkající se především operačních systémů a instalace opravných balíčků, kde hlavním cílem je udržet systém v aktuálním stavu a s nainstalovanými aktuálními softwarovými komponentami.
      20. **Hotline podpora** - jde oslužbu zajišťující poradenství po telefonu nebo elektronické komunikaci
      21. **Maintenance –** jedná se o zajištěnínových a opravných verzí software (včetně hlavních verzí), nových verzí firmware, přístupu k technické podpoře výrobcea přístupu k databázi řešených problémů.
      22. **Profylaxe -** profylaxe zahrnuje aktualizace firmware zařízení, aktualizace administrátorských nástrojů, kontrolu logů, kontrolu vytížení a využití, kontrolu kapacit.
    1. Obecná pravidla provozu
       1. Provozem se rozumí chod a udržování jednotlivých částí řešení, tj. hardware, systémový software, vybrané aplikace, technické infrastruktury, aktuální dokumentace.
       2. Informační systémy Zadavatele jsou provozovány v nepřetržitém provozu s výjimkou neočekávaných událostí a plánovaných odstávek.
       3. Veškeré technologie jsou umístěny v technologických místnostech KKN. Fyzický přístup do technologických místností je řízen interní směrnicí. Vstup je zajištěn uzamčením místnosti standardním zámkem či elektronickým zámkem. Pravidla přístupu budou vítěznému Uchazeči předána při podpisu smlouvy.
       4. Pravidelné profylaktické prohlídky probíhají v souladu s harmonogramem plánovaných profylaxí a odstávek, který je sestavován v rámci poskytování konkrétních služeb a je pravidelně předkládán ke schválení oprávněné osobě Zadavatele.
       5. Zásahy, které musí být provedeny mimo dobu profylaxe, jsou přednostně prováděny mimo provozní dobu příslušné služby. O nutnosti zásahů v provozní době služby rozhoduje projektový manažer Uchazeče a 48 hodin předem o nich informuje uživatele. Pokud je nevyhnutelně nutné provést zásah okamžitě, operátor Helpdesku a vedoucí OIT KKN jsou o této skutečnosti neprodleně informováni.
       6. Neplánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 1 hodinu před zahájením poskytování služby nebo činnosti.
       7. Plánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 24 hodin před zahájením poskytování služby nebo činnosti.
    2. Harmonogram poskytování služeb
       1. V průběhu poskytování služeb je Uchazeč povinen sestavovat harmonogram plánu poskytovaných služeb a činností. Harmonogram bude připravován vždy na dobu nejméně 3 měsíců dopředu.
       2. Harmonogram bude obsahovat časový rozvrh služeb a činností, případně jejich částí, které mají pravidelný charakter (profylaxe, údržba apod.), případně které jsou předvídatelné (instalace patchů, upgradů atd.).
       3. Všechny provozní činnosti musí být přednostně prováděny v době minimální zátěže dotčených systémů.
    3. Specifikace rozsahu podpory provozu
       1. Základní rozsah systémové podpory v rámci měsíčního paušálu:
          1. Pravidelné servisní prohlídky a revize předepsané výrobci
          2. Průběžné monitorování Prvků IT pokrývaných touto smlouvou, popř. dalších Prvků IT, které mohou ovlivnit jejich chod a které byly identifikovány v rámci předimplementační analýzy. Počet sledovaných parametrů nesmí být prakticky omezen, administrátoři KKN musí mít přístup ke sledovaným parametrům alespoň v režimu čtení.
          3. Řešení Incidentů dle podmínek SLA
          4. Profylaxe a patch management
          5. Hotline podpora v režimu 9x5
          6. Odborná podpora v režimu 9x5
          7. Celkový rozsah služeb Hotline podpora a Odborná podpora v rámci měsíčního paušálu je 6 hodin ve složení - 2 hodiny pro každou Komoditu (celkem 6 hodin).
          8. Helpdeskový systém s on-line přístupem (web, e-mail) pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
          9. Servisní dispečink pro telefonické zadávání požadavků dostupný v pracovní dny 8 -17 hod.
       2. Pro případ, že bude Zadavatel požadovat služby Hotline podpory nebo Odborné podpory podle odstavců (1)(e) a **Chyba! Nenalezen zdroj odkazů.** (např. konzultace, servisní zásahy, instalace, konfigurace, řešení problémů atp.) nad rámec uvedeného rozsahu služeb zahrnutých v měsíčním paušálu - viz. (1)(g), budou tyto služby hrazeny na základě počtu hodin realizovaných služeb dle hodinové sazby, Uchazeč nacení tyto služby v položkovém rozpočtu ve formě hodinové sazby za služby (označení služby „EXP-WRK“).
       3. Detailní specifikace požadavků a jejich rozsah pro jednotlivé kategorie prvků IT jsou v katalogových listech,
    4. Předávání informací o poskytované službě (reporting)
       1. Uchazeč zpracuje a poskytne Zadavateli každý měsíc souhrn informací o poskytovaných službách (report), ve kterém je popsán průběh realizace plnění za uplynulé období, včetně přehledu dodržování SLA parametrů, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti a dostupnosti systémů a prevenci incidentů.
       2. Souhrn informací o poskytovaných službách (report) bude obsahovat informace o jednotlivých službách a jejich provádění (dle povahy jednotlivých služeb a definice dle katalogových listů služeb).
       3. Měsíční report bude vyhotovován výhradně v elektronické formě a bude obsahovat souhrn činností provedených za vykazované období.
       4. Report bude za příslušné období vždy obsahovat minimálně:
  1. Informace o provedených změnách na Prvcích IT spojených s poskytováním služby.
  2. Informace o bezpečnostních incidentech zjištěných v souvislosti s poskytováním služby.
  3. Požadavek na součinnosti Zadavatele, požadované Uchazečem, k tomu, aby mohl dostát svým závazkům v poskytování předmětné služby.
     1. Způsob poskytování plnění
        1. Plnění je poskytováno zejména následujícím způsobem:
           1. Prostřednictvím pracovníka Uchazeče přímo na pracovišti Zadavatele
           2. Prostřednictvím pracovníka Uchazeče Vzdálenou správou
           3. Prostřednictvím pracovníka Uchazeče formou vzdálené konzultace
           4. Po dohodě smluvních stran automatizovanými nástroji při Monitorování, umožňují-li to technické prostředky na straně Zadavatele
        2. Uchazeč provede písemný záznam o provedení Služby na pracovišti Zadavatele, který předá Zadavateli a nechá si ho od něj potvrdit. Servisní služby, které jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.
        3. Zadavatel je povinen zabezpečit Uchazeči podmínky pro řádné plnění, zejména
           1. v případě Monitorování a Vzdálené správy zajistit a udržovat podmínky pro Vzdálený přístup Uchazeče k Prvkům IT,
           2. zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele,
           3. zajistit přístup k Provoznímu prostředí, který je nezbytný pro poskytování Služeb, včetně přístupu do prostor v objektu, kde je předmětný Prvek IT umístěn, případně přístup do prostor, v nichž jsou umístěna zařízení související s podporovaným systémem,
           4. zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku Uchazeče veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,
           5. umožnit Uchazeči v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,
           6. zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné.
        4. V případě, že nebudou uvedené podmínky Zadavatelem prokazatelně zabezpečeny, lhůta pro vyřešení případného Incidentu se zastaví a počítat se bude až po obnovení zabezpečení uvedených podmínek.
        5. Uchazeč je v případě potřeby též z vlastní iniciativy oprávněn požádat Zadavatele o dodatečné údaje o Incidentu a o nezbytnou součinnost Zadavatele na řešení Incidentu, bez které nelze zahájit či pokračovat v řešení Incidentu. Tím se zastavuje započítávání času, což je rozhodující pro určení čistého času řešení Incidentu při hodnocení úrovně poskytovaných služeb (SLA).
        6. Zadavatel je povinen
           1. písemně či elektronicky potvrdit Uchazeči provedení služby,
           2. zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeba a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,
           3. poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí, nejpozději do tří (3) Pracovních dnů po jejich písemném či ústním vyžádání, pokud se o obě strany nedohodnou jinak.
     2. Přítomnost pracovníků
        1. V průběhu běžné pracovní doby organizace bude v lokalitě Zadavatele (on-site) přítomen technik Uchazeče, který bude schopen řešit incidenty při provádění upgradů kritických prvků (datová základna - databázový stroj)). Přítomnost technika vždy bude stanovena po vzájemné dohodě v předstihu nejméně 10 pracovních dnů předem.
     3. Postup při řešení požadavků
        1. Zadavatel bude Požadavek oznamovat Uchazeči bez zbytečného odkladu jedním ze způsobů a na kontaktních místech uvedených ve Smlouvě o zabezpečení provozu, kam budou mít zajištěny přístup pověřené osoby Zadavatele. Momentem nahlášení požadavku Zadavatelem na hot-line nebo zadáním požadavku do HelpDesk začíná běžet lhůta pro Dobu odezvy.
        2. Součástí nahlášení požadavku Zadavatelem musí být:
           1. navrhovaná kategorizace a závažnost,
           2. popis Incidentu nebo Požadavku,
           3. jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh,
           4. kontaktní osoba.
        3. Uchazečem používaný systém pro HelpDesk bude pokrývat uvedené informace pro nahlášení požadavku.
        4. Incidenty budou před jejich nahlášením začleněny do skupin, viz dále a dle těchto skupin bude Uchazeč přistupovat k jejich řešení:

|  |
| --- |
| Incident/vada kategorie A |
| Prvek IT/služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody. |
| Incident/vada kategorie B |
| Prvek IT/služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz. |
| Incident/vada kategorie C |
| Ostatní - drobné incidenty/vady, které nespadají do kategorií A a/nebo B a které nejsou způsobeny software třetích stran. |
| Incident/vada kategorie D |
| Incidenty/vady, které jsou způsobeny software třetích stran. |

* + - 1. Uchazeč potvrdí obdržení požadavku dle podmínek SLA a bez ohledu na způsob nahlášení provede evidenci Požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.
      2. Uchazeč v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že Uchazeč v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení - zároveň přeřadí Incident do kategorie D a pokračuje v řešení v režimu BE (Best Effort).
      3. Zjistí-li Uchazeč v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele. Výskyt neodstranitelného Incidentu může být ze strany Zadavatele považován za podstatné porušení této smlouvy v případech, že Incident byl způsoben předchozím přímým jednáním Uchazeče, pokud o nich mohl mít s vynaložením veškeré odborné péče povědomost.
      4. Zjistí–li Uchazeč v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je Uchazeč povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy Uchazečem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.
      5. Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok Uchazeče na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.
      6. V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:
         1. čase vyřešení požadavku,
         2. v případě Incidentu specifikuje příčinu (pokud je známa),
         3. vyzve iniciátora k ověření funkčnosti služby.
      7. Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.
      8. Po vyřešení požadavku Uchazeč požadavek uzavře v systému HelpDesk a informuje Zadavatele. V případě Incidentu kategorie A zasílá návrh opatření pro snížení nebo eliminaci možnosti opakování stejného Incidentu.
      9. Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu Prvku IT; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu Prvku IT, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.
    1. Podmínky SLA
       1. Uchazeč se zavazuje dodržovat při řešení požadavků následující parametry (SLA).

|  |  |  |  |
| --- | --- | --- | --- |
| Kategorie incidentu | Garantovaná doba přijetí a akceptace hlášeného incidentu | Garantovaná doba zahájení prací na řešení incidentu po řádném nahlášení | Garantovaná doba ukončení incidentu po řádném nahlášení |
| A | 15 min | 6 hod | Nejpozději do 24 hod |
| B | 15 min | 8 hod | NBD |
| C | 15 min | NBD | 5BD |
| D | 15 min | NBD | BE |

* + - 1. Pro předání požadavků na plnění závazků vyplývajících z SLA je požadováno použití technologie umožňující nepřetržitý dálkový přístup v českém jazyce.
      2. Servisní kalendář (časový interval poskytování služeb) je stanoven min. v rozsahu 9x5 (8–17) v pracovních dnech, není-li u konkrétní služby uvedeno jinak.
      3. V rámci vymezení předmětu SLA Uchazeč nejlépe v technické příloze dostatečně přesně popíše, jaké služby a činnosti Zadavatele jsou pro plnění SLA zcela zásadní a kritické, respektive na jakých aplikacích a službách je provoz systémů závislý. Dále Uchazeč popíše, jakým způsobem zajistí dosažení podmínek SLA, možnosti měření SLA a možnosti ověření dosahování SLA, které bude mít Zadavatel k dispozici.
      4. Provozní činnosti budou kontrolovány Zadavatelem (nebo jím stanoveným subjektem) v rámci systému monitoringu.
    1. Seznam prvků IT

Následující tabulka obsahuje seznam Prvků IT, u nichž je požadováno Zabezpečení provozu

|  |  |  |
| --- | --- | --- |
| **Prvky IT** | | |
| **Prvek** | **Popis** | **Počet** |
| **Hardware** | | |
| - | není součástí dodávky | 0 |
| **Software** | | |
| 1 | Systémový software – virtuální servery, operační systémy | 4 |
| 2 | Systémový software - databázový server | 1 |
| 3 | Aplikační software - Systém pro správu identit | 1 |
| 4 | Aplikační software - Systém pro správu provozních dokumentů | 1 |
| 5 | Aplikační software – Systém pro řízení virtuálních desktopů | 1 |

* + 1. Záruky a servisní podmínky
       1. Záruka na veškeré servisní služby provedené v rámci zajištění provozu podpor v délce trvání 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.
  1. Katalogové listy
     1. Katalogový list S1.1 - Podpora provozu systému pro správu identit

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| KATALOGOVÝ LIST | | | | | | | | | | | | | | |
| OZNAČENÍ SLUŽBY | | S-APP-IDM | | | | | | | KÓD | | | S1.1 | | |
| Název služby | Podpora provozu systému pro správu identit | | | | | | | | | | | | | |
| VYMEZENÍ SLUŽBY | | | | | | | | | | | | | | |
| Prostředí | PRODUKČNÍ | | | | | | | | | | | | | |
| Cílová skupina | Centrální systémy, aplikace, uživatelé | | | | | | | | | | | | | |
| Požadované role obsazované Dodavatelem | Název role | | | | ID role | | Předpokládaný rozsah alokace (z provozní doby) | | | | | | Dostupnost | |
| Architekt | | | | IDM-AR | | 5% | | | | | | 8-17 | |
| Administrátor | | | | IDM-AD | | 20% | | | | | | 8-17 | |
| Manažer bezpečnosti | | | | IDM-BZ | | 10% | | | | | | 8-17 | |
| CENY | | | | | | | | | | | | | | |
| Položka | | | Cena bez DPH | | | Částka DPH | | | | | Cena s DPH | | | |
| Cena za podporu provozu | | | 55 810 Kč | | | 11 720 Kč | | | | | 67 530 Kč | | | |
| ROZSAH POŽADOVANÝCH ČINNOSTÍ | | | | | | | | | | | | | | |
| 1. Provoz systému IDM:    1. kontrola stavu všech komponentů systému – komodita K1 zakázky    2. kontrola služeb (na denní bázi),    3. kontrola logů,    4. kontrola monitoringu služby (na denní bázi),    5. kontrola výkonu/odezvy služeb systému (na denní bázi),    6. kontrola alokace zdrojů CPU, paměť, úložiště, komponenty systému (na denní bázi),    7. profylaktické činnosti,    8. návrh preventivních opatření vyplývající z monitoringu a profylaktických činností s cílem předejít možným výpadkům a omezením služby,    9. vyhodnocení a řešení funkčních a výkonnostních problémů systému,    10. provádění servisních a diagnostických služeb při závadě systému,    11. odborná technická podpora a odstraňování závad v předmětné oblasti,    12. provádění záloh dotčeného komponentu/serveru před každou změnou,    13. zálohování bude prováděno centrální službou Zadavatele,    14. vedení provozního deníku služby. 2. Správa systému IDM:    1. kontrola dostupnosti aktualizací a nových verzí software a dalších opravných balíků výrobce (na měsíční bázi),    2. údržba služby – všech komponentů řešení,    3. analýza vhodnosti a potřebnosti implementace opravného / aktualizačního balíku,    4. návrh opatření a postupu implementace opravného / aktualizačního balíku ke schválení Zadavateli,    5. předkládání návrhů na optimalizaci služby (na kvartální bázi),    6. instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna souhrnně v termínech dle závažnosti, nejdéle 1x kvartálně), 3. Zajištění maintenance:    1. Zajištění a dodávka maintenance (nových a opravných verzí software a aktualizací) systému IDM v rámci smluvního paušálu,    2. Zajištění a dodávka legislativních aktualizací pro zajištění shody systému IDM s platnou legislativou v rámci paušálu 4. Správa a aktualizace provozní dokumentace v rozsahu:    1. provozní deník služby – osoba, číslo požadavku z SD systému, popis prováděné činnosti, výsledek činnosti (úspěch/selhání), doba trvání)    2. aktuální přehled a schéma infrastruktury služby,    3. aktuální konfigurace komponentů služby,    4. aktuální přehled provozních parametrů služby,    5. správa konfigurací předmětné služby, 5. Účast na jednání provozních a pracovních týmů Zadavatele (1x měsíčně, na výzvu Zadavatele) | | | | | | | | | | | | | | |
| SERVICE LEVEL AGREEMENT (SLA) | | | | | | | | | | | | | | |
| Vyhodnocovací období | 1 kalendářní měsíc | | | | | | | | | | | | | |
| SLA PARAMETRY | | | | Jednotka | | | | Hodnota | | Max počet za období | | | |  |
| Dostupnost | | | | [%/měs] | | | | 98 | | N/A | | | |  |
| Provozní doba zaručená | | | | [hod-hod] | | | | 8–17 (9x5) | | N/A | | | |  |
| Max. doba výpadku | | | | [hod] | | | | 4 | | N/A | | | |  |
| Max. doba nedostupnosti dat | | | | [hod] | | | | 4 | | N/A | | | |  |
| Max. doba servisní odezvy | | | | [min] | | | | 15 | | N/A | | | |  |
| Odstranění výpadku – A | | | | [hod] | | | | 2 | | 1 | | | |  |
| Odstranění výpadku – B | | | | [dny] | | | | 1 | | 5 | | | |  |
| Odstranění výpadku – C | | | | [dny] | | | | 5 | | 10 | | | |  |
| Upřesnění kategorií incidentů a závad (zpřesnění globálních definic daných servisní smlouvou) | | | | | | | | | | | | | | |
| Kategorie A | Nefunkčnost systému | | | | | | | | | | | | | |
| Kategorie B | Snížený výkon či odezva služby | | | | | | | | | | | | | |
| Kategorie C | Ostatní závady nespadající do kategorie A nebo B. | | | | | | | | | | | | | |
| Způsob kontroly | | | | | | | | | | | | | | |
| Do dostupnosti jsou počítány pouze incidenty typu A, incidenty kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují. Měření parametrů služby budou prováděna v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost služeb terminálové farmy ve všech lokalitách. Měření bude prováděno jako součást monitoringu. | | | | | | | | | | | | | | |
| PODMÍNKY A OMEZENÍ SLUŽBY | | | | | | | | | | | | | | |
| Měrná jednotka provozu služby | Počet systémů pro správu identit | | | | | | | | | | | | | |
| Limit objemu služby |  | | | | | | | | | | | | | |
| Omezení | Předmětem služby není zajištění provozu klientských koncových zařízení a podpora uživatelů aplikací. | | | | | | | | | | | | | |
| Další podmínky | Povinnost poskytnout součinnost Zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně tohoto katalogového listu a nápravě zjištěných nedostatků. | | | | | | | | | | | | | |
| KRÁTKÝ POPIS STAVU PROSTŘEDÍ | | | | | | | | | | | | | | |
| Počet systémů IDM - 1 | | | | | | | | | | | | | | |

* + 1. Katalogový list S1.2 - Podpora provozu systému pro správu provozních dokumentů

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| KATALOGOVÝ LIST | | | | | | | | | | | | | | |
| OZNAČENÍ SLUŽBY | | S-APP-DMS | | | | | | | KÓD | | | S1.2 | | |
| Název služby | Podpora provozu systému pro správu provozních dokumentů | | | | | | | | | | | | | |
| VYMEZENÍ SLUŽBY | | | | | | | | | | | | | | |
| Prostředí | PRODUKČNÍ | | | | | | | | | | | | | |
| Cílová skupina | Centrální systémy, aplikace, uživatelé, správci majetku | | | | | | | | | | | | | |
| Požadované role obsazované Dodavatelem | Název role | | | | ID role | | Předpokládaný rozsah alokace (z provozní doby) | | | | | | Dostupnost | |
| Architekt | | | | DMS-AR | | 5% | | | | | | 8-17 | |
| Administrátor | | | | DMS-AD | | 20% | | | | | | 8-17 | |
| Manažer bezpečnosti | | | | DMS-BZ | | 5% | | | | | | 8-17 | |
| CENY | | | | | | | | | | | | | | |
| Položka | | | Cena bez DPH | | | Částka DPH | | | | | Cena s DPH | | | |
| Cena za podporu provozu | | | 20 905 Kč | | | 4 390 Kč | | | | | 25 295 Kč | | | |
| ROZSAH POŽADOVANÝCH ČINNOSTÍ | | | | | | | | | | | | | | |
| 1. Provoz systému DMS:    1. kontrola stavu všech komponentů systému – komodita K2 zakázky    2. kontrola služeb (na denní bázi),    3. kontrola logů (na denní bázi),    4. kontrola monitoringu služby (na denní bázi),    5. kontrola výkonu/odezvy služeb systému (na denní bázi),    6. kontrola alokace zdrojů CPU, paměť, úložiště, komponenty systému (na denní bázi),    7. profylaktické činnosti,    8. návrh preventivních opatření vyplývající z monitoringu a profylaktických činností s cílem předejít možným výpadkům a omezením služby,    9. vyhodnocení a řešení funkčních a výkonnostních problémů systému,    10. provádění servisních a diagnostických služeb při závadě systému,    11. odborná technická podpora a odstraňování závad v předmětné oblasti,    12. provádění záloh dotčeného komponentu/serveru před každou změnou,    13. zálohování bude prováděno centrální službou Zadavatele,    14. vedení provozního deníku služby. 2. Správa systému DMS:    1. kontrola dostupnosti aktualizací a nových verzí software a dalších opravných balíků výrobce (na měsíční bázi),    2. údržba služby – všech komponentů řešení,    3. analýza vhodnosti a potřebnosti implementace opravného / aktualizačního balíku,    4. návrh opatření a postupu implementace opravného / aktualizačního balíku ke schválení Zadavateli,    5. předkládání návrhů na optimalizaci služby (na kvartální bázi),    6. instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna souhrnně v termínech dle závažnosti, nejdéle 1x kvartálně), 3. Zajištění maintenance:    1. Zajištění a dodávka maintenance (nových a opravných verzí software a aktualizací) systému v rámci smluvního paušálu,    2. Zajištění a dodávka legislativních aktualizací pro zajištění shody systému IDM s platnou legislativou v rámci paušálu 4. Správa a aktualizace provozní dokumentace v rozsahu:    1. provozní deník služby – osoba, číslo požadavku z SD systému, popis prováděné činnosti, výsledek činnosti (úspěch/selhání), doba trvání)    2. aktuální přehled a schéma infrastruktury služby,    3. aktuální konfigurace komponentů služby,    4. aktuální přehled provozních parametrů služby,    5. správa konfigurací předmětné služby, 5. Účast na jednání provozních a pracovních týmů Zadavatele (1x měsíčně, na výzvu Zadavatele) | | | | | | | | | | | | | | |
| SERVICE LEVEL AGREEMENT (SLA) | | | | | | | | | | | | | | |
| Vyhodnocovací období | 1 kalendářní měsíc | | | | | | | | | | | | | |
| SLA PARAMETRY | | | | Jednotka | | | | Hodnota | | Max počet za období | | | |  |
| Dostupnost | | | | [%/měs] | | | | 98 | | N/A | | | |  |
| Provozní doba zaručená | | | | [hod-hod] | | | | 8–17 (9x5) | | N/A | | | |  |
| Max. doba výpadku | | | | [hod] | | | | 4 | | N/A | | | |  |
| Max. doba nedostupnosti dat | | | | [hod] | | | | 4 | | N/A | | | |  |
| Max. doba servisní odezvy | | | | [min] | | | | 15 | | N/A | | | |  |
| Odstranění výpadku – A | | | | [hod] | | | | 2 | | 1 | | | |  |
| Odstranění výpadku – B | | | | [dny] | | | | 1 | | 5 | | | |  |
| Odstranění výpadku – C | | | | [dny] | | | | 5 | | 10 | | | |  |
| Upřesnění kategorií incidentů a závad (zpřesnění globálních definic daných servisní smlouvou) | | | | | | | | | | | | | | |
| Kategorie A | Nefunkčnost systému | | | | | | | | | | | | | |
| Kategorie B | Snížený výkon či odezva služby | | | | | | | | | | | | | |
| Kategorie C | Ostatní závady nespadající do kategorie A nebo B. | | | | | | | | | | | | | |
| Způsob kontroly | | | | | | | | | | | | | | |
| Do dostupnosti jsou počítány pouze incidenty typu A, incidenty kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují. Měření parametrů služby budou prováděna v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost služeb terminálové farmy ve všech lokalitách. Měření bude prováděno jako součást monitoringu. | | | | | | | | | | | | | | |
| PODMÍNKY A OMEZENÍ SLUŽBY | | | | | | | | | | | | | | |
| Měrná jednotka provozu služby | Počet systémů pro správu pro správu provozních dokumentů | | | | | | | | | | | | | |
| Limit objemu služby |  | | | | | | | | | | | | | |
| Omezení | Předmětem služby není zajištění provozu klientských koncových zařízení a podpora uživatelů aplikací. | | | | | | | | | | | | | |
| Další podmínky | Povinnost poskytnout součinnost Zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně tohoto katalogového listu a nápravě zjištěných nedostatků. | | | | | | | | | | | | | |
| KRÁTKÝ POPIS STAVU PROSTŘEDÍ | | | | | | | | | | | | | | |
| Počet systémů DMS - 1 | | | | | | | | | | | | | | |

* + 1. Katalogový list S1.3 - Podpora systému řízení virtuálních desktopů

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| KATALOGOVÝ LIST | | | | | | | | | | | | | | |
| OZNAČENÍ SLUŽBY | | S-APP-TS | | | | | | | KÓD | | | | S1.3 | |
| Název služby | Podpora systému pro řízení virtuálních desktopů | | | | | | | | | | | | | |
| VYMEZENÍ SLUŽBY | | | | | | | | | | | | | | |
| Prostředí | PRODUKČNÍ | | | | | | | | | | | | | |
| Cílová skupina | Uživatelé, správci IT | | | | | | | | | | | | | |
| Požadované role obsazované uchazečem | Název role | | | | ID role | | Předpokládaný rozsah alokace (z provozní doby) | | | | | Dostupnost | | |
| Architekt | | | | TS-AR | | 5% | | | | | 8-17 | | |
| Administrátor | | | | TS-AD | | 15% | | | | | 8-17 | | |
| Manažer bezpečnosti | | | | TS-BZ | | 5% | | | | | 8-17 | | |
| CENY | | | | | | | | | | | | | | |
| Položka | | | Cena bez DPH | | | Částka DPH | | | | | Cena s DPH | | | |
| Cena za podporu provozu | | | 20 000 Kč | | | 4 200 Kč | | | | | 24 200 Kč | | | |
| ROZSAH POŽADOVANÝCH ČINNOSTÍ | | | | | | | | | | | | | | |
| 1. Provoz systému pro řízení virtuálních desktopů – komodita K3 zakázky:    1. Kontrola logů (na týdenní bázi),    2. Kontrola dostupnosti služby (na denní bázi),    3. Kontrola vysoké dostupnosti ověřovací platformy (na denní bázi),    4. Odborná technická podpora a odstraňování závad v předmětné oblasti, 2. Správa systému v serverové infrastruktuře    1. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných a aktualizačních balíků výrobce (na kvartální bázi) včetně analýzy vhodnosti a potřebnosti implementace opravného balíku,    2. návrh opatření a postupu implementace opravného balíku ke schválení Zadavateli,    3. předkládání návrhů na optimalizaci aktualizačních systémů infrastruktury (na kvartální bázi),    4. instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna souhrnně v termínech dle závažnosti, nejdéle 1x kvartálně),    5. implementace schválených požadavků na změnu konfigurace. 3. Součinnost s ostatními dodavateli související s návrhem změn v infrastruktuře. 4. Správa a aktualizace provozní dokumentace 5. Účast na jednání provozních a pracovních týmů Zadavatele (1x měsíčně, na výzvu Zadavatele) | | | | | | | | | | | | | | |
| SERVICE LEVEL AGREEMENT (SLA) | | | | | | | | | | | | | | |
| Vyhodnocovací období | 1 kalendářní měsíc | | | | | | | | | | | | | |
| SLA PARAMETRY | | | | Jednotka | | | | Hodnota | | Max počet za období | | | |  |
| Dostupnost | | | | [%/měs] | | | | 95 | | N/A | | | |  |
| Provozní doba zaručená | | | | [hod-hod] | | | | 8–17 (9x5) | | N/A | | | |  |
| Max. doba výpadku | | | | [hod] | | | | 8 | | N/A | | | |  |
| Max. doba nedostupnosti dat | | | | [hod] | | | | 8 | | N/A | | | |  |
| Max. doba servisní odezvy | | | | [min] | | | | 30 | | N/A | | | |  |
| Odstranění výpadku – A | | | | [hod] | | | | 8 | | 1 | | | |  |
| Odstranění výpadku – B | | | | [dny] | | | | 1 | | 5 | | | |  |
| Odstranění výpadku – C | | | | [dny] | | | | 5 | | 10 | | | |  |
| Upřesnění kategorií incidentů a závad (zpřesnění globálních definic daných servisní smlouvou) | | | | | | | | | | | | | | |
| Kategorie A | Chyba, která způsobí celkovou nedostupnost služby | | | | | | | | | | | | | |
| Kategorie B | Chyba snižující výkon či odezvu služby | | | | | | | | | | | | | |
| Kategorie C | Závady, které neomezí provoz služby a ostatní závady nespadající do kategorie A nebo B | | | | | | | | | | | | | |
| Způsob kontroly | | | | | | | | | | | | | | |
| Do dostupnosti jsou počítány pouze incidenty typu A, incidenty kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují. Měření parametrů služby budou prováděna v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost služeb serverů WSUS ve všech lokalitách. Měření bude prováděno jako součást monitoringu. | | | | | | | | | | | | | | |
| PODMÍNKY A OMEZENÍ SLUŽBY | | | | | | | | | | | | | | |
| Měrná jednotka provozu služby | Počet serverů systému | | | | | | | | | | | | | |
| Limit objemu služby |  | | | | | | | | | | | | | |
| Omezení | Služba nezahrnuje správu HW na serverech a provoz samotných aplikačních serverů na platformě MS Windows (SQL server, zálohovací systém atd.).  Služba se nevztahuje na klientské stanice a její součástí není podpora uživatelů. | | | | | | | | | | | | | |
| Další podmínky | Povinnost poskytnout součinnost Zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně tohoto katalogového listu a nápravě zjištěných nedostatků. | | | | | | | | | | | | | |
| KRÁTKÝ POPIS STAVU PROSTŘEDÍ | | | | | | | | | | | | | | |
| Počet serverů – 2 | | | | | | | | | | | | | | |

1. Popis postupu implementace předmětu plnění
   1. Obecné podmínky implementace

Následující podmínky vycházejí z obecných zásad řízení implementačních projektů a zahrnují zkušenosti uchazeče získané z velkého množství (stovky) projektů obdobného zaměření. Popis je použitými pojmy koncipován jako materiál nevyžadující formální vzdělání v oblasti projektového řízení a řízení IT služeb a orientuje se především na praktickou stránku a srozumitelnost implementačního postupu.

* 1. Řízení implementace

Z pohledu implementace bude uchazeč přistupovat k veřejné zakázce „Modernizace provozních IS“ jako k jednomu projektu složenému z více vzájemně provázaných částí – jednotlivých komodit. Výhodou toho přístupu pro zadavatele je jednotné řízení celého projektu jedním **projektovým manažerem**, který zajišťuje plnění smluvních a dalších sjednaných činností a koordinuje činnosti jednotlivých specialistů uchazeče a jeho subdodavatelů. Projektový manažer je tak hlavním komunikačním kontaktem pro zadavatele v oblasti organizace projektu – tímto způsobem jsou minimalizovány nároky na projektový tým zadavatele z pohledu komunikace a koordinace projektu. Projektový manažer dále zajišťuje dodržování časového harmonogramu, organizaci projektových a technických schůzek, pořizování a schvalování zápisů a pravidelný reporting o průběhu projektu – tyto činnosti tak probíhají v režii uchazeče a zadavatel jimi není zatěžován. Projektový manažer je správcem případných změnových požadavků navrhovaných uchazečem či zadavatelem. V případě potřeby je projektový manažer eskalačním kontaktem první úrovně.

Pro zajištění technické konzistence celého řešení a postupu bude v implementačním týmu ustanovena role **architekta řešení** – jde o technickou roli zastřešující odbornými znalostmi celou šíři implementovaného řešení a zajišťující optimální integraci (provázání) jednotlivých technologií a částí projektu (komodit) na technické úrovni. Architekt řešení je hlavním komunikačním kontaktem zadavatele v technických záležitostech - tímto způsobem jsou minimalizovány nároky na projektový tým zadavatele z pohledu komunikace a koordinace projektu v technických záležitostech.

* 1. Zajištění vysoké odbornosti implementace a přenosu know-how

Základní úroveň využití a uplatnění doporučených postupů výrobců bude zajištěna prováděním implementačních činností specialisty certifikovanými výrobci pro danou oblast implementace. Prokázání znalostí a pochopení implementačních postupů a pravidel spolu s prokázáním technických znalostí produktů a technologií je stěžejním cílem certifikačních procesů výrobců.

Vedle technických certifikací budou všichni specialisté uchazeče i jeho subdodavatelů disponovat praktickými zkušenostmi z implementací technicky i rozsahem obdobných projektů, které uplatní v analytické, návrhové i instalační fázi projektu. Zadavatel tak získá významnou přidanou hodnotu současně v několika oblastech:

* uplatnění osvědčených postupů a řešení z obdobných projektů (tzv. best practice)
* zkrácení všech fází projektu na minimum – eliminace nevhodných variant a postupů
* minimální zátěž projektového týmu zadavatele – předkládání konkrétních návrhů či malého počtu jasně vyhodnotitelných variant namísto dotazů
  1. Zajištění bezpečnosti

Kromě smluvního zajištění důvěrnosti dat a informací a obvyklého dodržování bezpečnostních norem a pravidel bude uchazeč v průběhu implementace klást důraz na následující oblasti bezpečnosti:

* zajištění kontinuity provozu – vzhledem k prostředí vyžadujícímu trvalý provoz IT technologií bude implementační tým nasazovat nové technologie tak, aby byl v případě potřeby schopen rychle obnovit předchozí (tzv. poslední funkční) stav
* zajištění technické ochrany dat – vzhledem k rozsáhlosti projektu a počtu změn bude uchazeč průběžně provádět zálohy dat

Dodavatele bude respektovat provozní podmínky zadavatele a činnosti vyžadující omezení provozu bude provádět v předem sjednaných časech, ve kterých bude omezení provozu zadavatele minimální. Dodavatel bude preferovat technologické postupy a řešení, které v maximální možné míře eliminují omezení provozu zadavatele a případné součinnostní kroky uživatelů či administrátorů (např. při migracích dat) umožní rozložit v čase tak, aby jejich vykonáváním nebyl omezen běžný provoz.

* 1. Implementační fáze projektu

Jednotlivé fáze projektu budou vycházet z doporučení ITIL, které pro zavádění ICT služeb (definuje následující procesy (fáze):

* Service Strategy
* Service Design
* Service Transition
* Service Operation
* Continual Service Improvement - CSI
  + 1. Analytická – Service strategy

V rámci této fáze proběhne požadovaná předimplementační analýza. Součástí fáze je úvodní technický workshop technických specialistů uchazeče a zadavatele. Náplní workshopu je moderovaná diskuze zaměřená na technickou stránku projektu – zejména detailní specifikaci cílů projektu a očekávání jeho příjemců/uživatelů. Důležitou částí je specifikace objektivních podmínek, pravidel a zvyklostí, v nichž bude projekt realizován.

V analytické části specialisté uchazeče detailně zdokumentují stávající stav IT infrastruktury a aplikací včetně konfigurací, verzí a vzájemných vazeb.

* + 1. Návrhová – Service design

Na základě zdokumentovaného stavu jednotliví specialisté pod vedením architekta řešení navrhnou detailní postupy dosažení cílového stavu včetně potřebných konfigurací jednotlivých technologií a nezbytných součinností zadavatele. V průběhu návrhu postupů budou zvažována rizika spojená s uplatněním postupu. V případě nezanedbatelného rizika bude součástí postup návrh na odstranění či zmírnění rizika. Postupy budou zpracovány do dokumentu Prováděcí dokumentace, který bude zadavateli prezentován a předán ke schválení. Po schválení Prováděcí dokumentace bude uchazeč podle této dokumentace realizovat instalační fázi projektu.

* + 1. Instalační - Service Transition

V rámci této fáze proběhne dodávka, montáž, oživení, konfigurace a otestování veškerých dodaných komponent (hw i sw) dle Prováděcí dokumentace. Pro zachování přehlednosti dokumentu neuvádíme popis této fáze jako soupis prováděných služeb dle Technické specifikace a potvrzení provedení každé z nich. Veškeré požadované služby budou uchazečem provedeny přesně dle poptávky. Pro prokázání jednoznačnosti navrženého implementačního postupu dále uvádíme chronologický seznam jednotlivých instalačních činností/kroků v doporučeném pořadí realizace, které povede k úspěšnému splnění předmětu plnění – je patrné, že projekt není vhodné (ani možné) implementovat v pořadí dle komodit a dokonce je nezbytné některé komodity implementovat ve více fázích proložených implementací jiné komodity. Všechny činnosti/kroky jsou řazeny sériově (za sebou), v průběhu implementace však budou některé z nich z důvodů urychlení implementace prováděny paralelně (souběžně), pokud to bude možné.

V rámci analytické, návrhové i implementační fáze pro všechny oblasti budou realizovány následující kroky Předimplementační anylýzy tak, aby byly beze zbytku naplněny cíle a očekávání Zadavatele vyplývající ze zadávací dokumentace:

1. Stávající stav (vstupy) relevantní pro návrh implementace komodity.
2. Způsob začlenění nabízených komodit do stávajícího prostředí.
3. Konfigurační změny nabízeného systému potřebné pro naplnění povinných požadavků.
4. Virtualizační infrastruktura (serverová, síťová, disková i aplikační) ve vztahu k plánovanému využití.
5. Integrace nabízených softwarových systémů.
6. Požadované součinnosti Zadavatele a jejich rozsah.
7. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Dále pak budou provedeny následující kroky pro zpracování Prováděcí dokumentace:

1. Popis cílového stavu / konfigurace nabízeného systému,
2. Detailní harmonogram realizace včetně uvedení kritických milníků,
3. Vazby na integrované systémy systémy,
4. Návrh akceptačních kritérií a akceptačních testů.
   * 1. K1 - Správa identit

Systém pro správu identit IDM zavede výrazně vyšší úroveň automatizace správy elektronických identit a integrace s klíčovými aplikačními systémy zadavatele. Při implementace komodity pro správu a řízení identit bude v rámci implementačního projektu zorganizována série workshopů na specifická témata řízení identit. Bude se jednat zejména o oblast představení možností a vlastností dodávaného systému IDM, představení možností napojení systému IDM na vybrané systémy zadavatele. Série workshopů bude zorganizována mezi týmem našich technických specialistů a vybraných klíčových specialistů na straně zadavatele. Cílem těchto workshopů bude získat od zadavatele veškeré potřebné informace pro vytvoření dokumentace analýzy zahrnující údaje potřebné k přípravě implementace IDM v prostředí zadavatele.

Analýza pro systém řízení identit bude zahrnovat následující části:

Analýza procesů a aplikací KKN se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí. V rámci této části naši specialisté zmapují stávající procesy a požadavky z oblasti správy identit na straně KKN. Konkrétně se jedná o procesy nástupu nového zaměstnance a přiřazení oprávnění v systémech, se kterými potřebuje zaměstnanec pracovat. Dále pak proces odchodu zaměstnance a deaktivace jeho přístupových účtů, změny organizačního začlenění zaměstnance, správa oprávnění pro externí subjekty, proces přiřazování a změny hesla, proces přiřazování a změny uživatelského jména, atd.

Analýza požadavků KKN zasílaných centrálním informačním systémům KKN.

Technologický popis stávajících technologií s vazbou na systém správy identit. V rámci této části naši specialisté zmapují stávající technologie a systémy s vazbou na systém správy identit. Jedná se zpravidla o technologie provozu IT infrastruktury zadavatele a jednotlivé systémy významné z hlediska správy identit jako personální systém, adresářová služba, emailový server, spisová služba a další. Naši specialisté rovněž provedou společně se zástupci specialistů ze strany zadavatele rozbor dat vázaných na správu identit v jednotlivých systémech zadavatele.

Analýza možností správy výstupních struktur. V rámci této části naši specialisté přestaví možnosti výstupních struktur systému. Jedná se zejména o reporty aplikačních rolí, historizační reporty identit, report pro ohlášení působnosti k nové agendě nebo agendové činností roli, simulační reporty platformy IDM atd.

Analýzu evidenčních údajů a logů. V rámci této části naši specialisté přestaví možnosti správy evidenční údajů v systému IDM a možnosti vytváření logů v systému IDM. Dále bude představena práce s logy systému IDM.

Návrh životního cyklu identity uživatelů. V rámci této části naši specialisté dle sesbíraných vstupů navrhnou proces životního cyklu identit platný pro zavedení systému IDM.

Model organizační struktury. V rámci této části naši specialisté zmapují stávající organizační strukturu na straně KKN. Bude proveden rozbor jednotlivých částí organizační struktury a jejich částí – odbory, oddělení včetně toho, ve kterých systémech je organizační struktura spravována a jakými způsoby.

Seznam systemizovaných pracovních pozic a přiřazení pracovníků k pracovním pozicím. V rámci této části naši specialisté zmapují stávající hierarchii systematizovaných stávajících pozic na straně KKN. Bude proveden rozbor jednotlivých vazeb nadřízenosti a podřízenosti pracovních pozic, obsazenost pracovních pozic, mechanizmy změn nastavení pracovních pozic. Bude přestaven návrh navazovat uživatelská oprávnění na pracovní pozice.

Atributy poskytované personálním systémem v souladu s potřebami obsluhovaných systémů a návrh jejich využití. V rámci této části naši specialisté zmapují údaje spravované v personálním systém (evidence organizační struktury, pracovních pozic, osob). Bude proveden rozbor, zda jsou tato data dostatečná pro řízení oprávnění systémem IDM napříč systémy KKN a centrálními systémy.

Manažerský souhrn vhodný pro prezentaci výstupů analýzy vedení KKN. V rámci předimplementační analýzy bude vypracován manažerský souhrn obsahující hlavní body vyplývající z analýzy stávajícího stavu včetně návrhu metodických, procesních a technických opatření pro implementaci systému IDM.

Výstupy z jednotlivých částí budou zpracovány do dokumentu Přeimplementační analýza, který bude zadavateli prezentován a předán ke schválení. Po schválení této dokumentace bude uchazeč podle této dokumentace realizovat návrhovou fázi projektu. V rámci návrhové fáze uchazeč vypracuje prováděcí dokumentaci popisující návrh cílového stavu implementace systému IDM. Dokumentace bude vycházet z dokumentace předimplementační analýzy a bude zahrnovat následující části:

Návrh implementace systému IDM. V rámci této části naši specialisté popíší návrh implementace systém IDM pro KKN. V návrhu řešení implementace IDM bude zohledněn navržený cyklus správy identit z dokumentace přeimplementační analýzy a další vstupy z předimplementační analýzy. Návrh implementace systému IDM bude obsahovat návrh a konfiguraci implementovaného systém IDM, návrh implementace algoritmu pro správu uživatelský jmen, hesel a dalších potřebných nastavení systému IDM.

Návrh napojení na požadované systémy ze strany KKN. V rámci této části naši specialisté popíší návrh implementace napojení systému IDM na požadované systémy ze strany KKN. U každého popisovaného napojení bude uveden směr synchronizace dat mezi systém IDM a požadovanými systémy, rozsah synchronizovaných dat, režimy synchronizace a tabulka mapování a transformace údajů, atributů přenášených v rámci jednotlivých synchronizací.

Návrh a provedení akceptačních testů. V rámci této části naši specialisté popíší detailní návrh akceptačních kritérií, které budou obsahovat návrh výkonových, integračních a testů případů užití systému IDM.

Návrh požadovaných úprav stávajících systémů. Při implementaci systému IDM a jeho napojení na systémy v organizaci je zpravidla nutné zajistit úpravu dat a provedení instalace potřebných komponent na straně třetích systémů. V rámci této fáze budou vydefinovány požadavky na úprav těchto dat případně systémů pro dosažené metodicky vhodného a konzistentního stavu dat požadovaného pro řízení identit.

V rámci instalační fáze komodity pro správu a řízení identit budou provedeny následující aktivity:

Příprava implementačního balíku IDM. V rámci této aktivity naši specialisté připraví implementační balík pro provedení instalace systému IDM v prostředí KKN. Tento instalační balík vznikne na základě podkladů a dokumentace předimplementační analýzy a prováděcí (návrhové) dokumentace. Instalační balíček bude následně otestován našimi specialisty v našem interním vývojovém a testovacím prostředí.

Provedení nezbytných součinností na straně napojovaných systémů ze strany IDM. Při implementaci systému IDM a jeho napojení na systémy v organizaci je zpravidla nutné zajistit úpravu dat a provedení instalace potřebných komponent na straně třetích systémů. V rámci této fáze budou vydefinovány požadavky na úpravu dat těchto systémů pro dosažení metodicky vhodného a konzistentního stavu požadovaného pro řízení identit.

Instalace IDM do prostředí KKN. V rámci této aktivity naši specialisté nainstalují připravený instalační balík do prostředí KKN. Dále bude zajištěno ve spolupráci se zadavatelem a dodavateli systémů třetích stran provedení požadovaných úprav dat v systémech KKN pro efektivní řízení identit.

Provedení testů systému IDM. V rámci této aktivity naši specialisté provedou testy systému IDM v prostředí KKN. Následně budou ve spolupráci s KKN provedeny akceptační testy řešení IDM.

Provedení simulačních synchronizací. V rámci této aktivity naši specialisté provedou simulační synchronizace systému IDM v prostředí KKN na požadované napojované systémy. Výstupem této aktivity budou vytvořeny rozdílové reporty poukazující na případné nekonzistence identitních dat v jednotlivých napojovaných systémech. Následně budou ve spolupráci s KKN provedeny aktivity pro odstranění případných datových nekonzistencí.

Spuštění řádných pravidelných synchronizací. Po uvedení identitních dat do souladu v rámci předchozí aktivity, bude možné za naší asistence nastavit úlohy pravidelných automatických synchronizací IDM s požadovanými systémy.

Doporučené postupy

Pro kvalitní návrh a implementaci systému IDM budou využity osvědčené a doporučené postupy (tzn. best practice – nejlepší praktiky).

Správa uživatelských rolí. V rámci řízení oprávnění IDM umožňuje centrální správu uživatelských rolí, tj. zařazení uživatele do odpovídající role v daném systému nebo aplikaci. Aplikační role je možné v IDM přiřazovat na koncové uživatele. IDM navíc umožňuje přiřazovat aplikační role na systematizovaná místa, organizační jednotky a skupiny. Aplikační role přiřazené na tyto referenční údaje následně „propadávají“ na koncové uživatele, kteří jsou na daných organizačních jednotkách, systematizovaných místech a skupinách včleněni. Mechanismus implementovaných konektorů pak zajištuje, že jsou identity a jejich změny včetně odpovídajících rolí a oprávnění vypropagovávány z IDM do relevantních systémů a to v odpovídajícím formátů a rozsahu definovaném pro každý jednotlivý systém samostatně.

Import aplikací a aplikačních rolí. IDM umožňuje správu číselníku aplikací a dále pak správu číselníku aplikačních rolí pro dané aplikace. V IDM je možné aplikační role evidovat a spravovat ručně přes portál. Dále je možné do IDM synchronizovat seznam aplikačních rolí přes rozhraní webových služeb IDM. Služba importu aktualizuje aplikace a aplikační role požadované skupiny aplikací. V případě, že není zadána na vstupu skupina aplikací, tak je aktualizována pouze samostatná aplikace. V případě, že je na vstupu předaná skupina aplikací, která neexistuje, vytvoří se nová skupina aplikací. Je-li v seznamu aplikací nová aplikace dosud nezaevidovaná v IDM, vytvoří se v IDM nový záznam. Chybějící aplikace se automaticky nedeaktivují. Pro aplikační role příslušné aplikace platí, že nové role na vstupu se vytvoří v IDM, chybějící se deaktivují.

Správa skupin a členství v skupinách adresářové služby. IDM umožňuje správu skupin a správu členství v skupinách adresářové služby. IDM umožňuje evidenci skupin, které mohou, ale nemusí být synchronizovány s adresářovými službami jako například Active Directory, LDAP, atd. V IDM je možné následně začleňovat jednotlivé identity do těchto skupin buď ručně v portálu IDM nebo automaticky podle definovaných pravidel. IDM umožňuje následně synchronizovat skupiny a členství ve skupinách do cílové adresářové služby. IDM dále umožňuje iniciační načtení seznamu skupin a uživatelských účtu z adresářové služby pro naplnění evidence v IDM.

Automatické zařazení uživatelů do skupin a aplikační rolí. Kromě ručního zařazení uživatele do skupiny administrátorem IDM může být uživatel při zápisu změn zařazen do skupin uplatněním pravidel pro automatické zařazení do skupin a aplikačních rolí. Pro automatické zařazení nastaví administrátor v administrátorské konzoli pravidel - sadu pravidel, podle kterých se na základě atributů uživatele vyhodnotí sada uživatelských skupin, aplikačních rolí, do kterých má být uživatel zařazen. Automatické zařazení uživatele do skupiny může být nastaveno podle různých atributů uživatele – např. zařazení do organizační jednotky, na pracovní místo a dalších atributů resp. kombinace atributů uživatele. Spouštění pravidel je definováno jako synchronizovaný systém, do něhož lze nastavit interval spuštění změnové nebo kompletní synchronizace (vyhodnocení pravidel). Na základě vyhodnocení sady pravidel se uživatelé zařadí do příslušných skupin, aplikačních rolí. Ruční zařazení do skupiny (administrátorem) má přednost před automatickým zařazením a není automatickým procesem dotčeno. Uživatelsky (administrátorem) je možné přepnout příznak automatického / ručního zařazení.

Výsledné stavy vyhodnocení pravidel:

* Beze změny
* Nové skupiny, role – uživatel se zařadí
* Chybějící skupiny, role – uživatel se vyjme. Nelze automaticky vyjmout ze skupiny nebo role, která má „automaticky = false“.

Změna zařazení do skupiny se promítne s okamžitou platností – po aplikaci pravidel.

Stupně komunikace IDM s připojenými systémy. Řešení IDM umožní spravovat životní cyklus všech identit v rámci infrastruktury zadavatele. Napojení jednotlivých IS a aplikací IDM může být implementováno v následujícím rozsahu:

* Plná integrace (správa identit) – kompletní správa identit včetně nastavení konkrétních práv a rolí probíhá pouze v systému IDM a IS či aplikace přebírá toto nastavení, např. procesy založ, edituj, smaž uživatele, aktivuj/deaktivuj přístup, přiřaď/odeber konkrétní roli a práva.
* Částečná (poloautomatická) správa – v IDM se nastavují přístupové údaje uživatele (založ, edituj, smaž, zablokuj), v integrovaném IS či aplikaci se definují konkrétní role a práva.
* Nepřipojené (virtuální) aplikace – za využití IDM je požádáno o založení/změnu/smazání přístupu, rolí a práv, nastavení je však nutné provést „ručně“ administrátorem – aplikace není přímo integrována. IDM obsahuje notifikační konektor, který bude simulovat napojení aplikace, která zatím není napojena na IDM. Pokud administrátor nebo automatické pravidlo přidají nebo odeberou identitě roli v IDM z této aplikace nebo změní identitu, pošle se emailová notifikace definovanému příjemci (administrátorovi) aplikace. Příjemce následně může na základě této notifikace provést požadované nastavené v dané aplikaci.

IDM rovněž implementuje plnou integraci s adresářovou službou včetně správy skupin, organizačních jednotek a příslušnosti uživatelů do těchto objektů. V případě, že jednotlivé aplikace využívají pro řízení autentizace a autorizace adresářové služby, tak je možné přes IDM tímto způsobem řídit plnou nebo částečnou správu identit i v těchto aplikacích.

* + 1. K2 – Správa provozních dokumentů

V rámci projektu bude využito stávajícího řešení zadavatele ALVAO a bude provedena jeho parametrizace dle požadavků ZD pro řízení požadovaných procesů.

Architektura nabízeného řešení bude v souladu s doporučením výrobce - viz odkaz <https://doc.alvao.com/support/doc/cs/alvao_10_0/alvao_service_desk/implementation/architecture.aspx> Systém ALVAO využívá operačního systému MS Windows Server, který je plně kompatibilní se stávajícím prostředím a webových služeb na bázi Microsoft IIS.

Produkty ALVAO jsou vyvíjeny v souladu s principy a doporučeními ITIL. Informační systém ALVAO byl certifikován mezinárodní certifikační autoritou Pink Elephant na použití šesti nejvíce využívaných ITIL procesů. Následně byl ověřen společností AXELOS, která dnes stojí za standardem ITIL, jako doporučený nástroj na nejvyšší úrovni GOLD a tím se zařadil mezi 5 nejlepších nástrojů na celém světě. Viz <https://www.alvao.cz/alvao-top5-itil-nastroji-celeho-sveta/>

Microsoft Active Directory slouží jednak jako zdroj informací o uživatelích a organizačních útvarech, ale také jako jednotné místo, které řídí uživatelské role a oprávnění v systému. Tato nativní integrace ve svém důsledku významně snižuje administrativní úkony spojené s provozováním a udržováním systému. Implementace řešení nijak negativně neovlivní chod stávajícího prostředí.

Systém bude integrován s MS Outlook (2010 a vyšší).

Sytém bude integrován s HELIOS Green pro získávání potřebných údajů

V rámci projektu bude dodána detailní uživatelská a administrátorská dokumentace (včetně popisů API a jeho použití) verzi.

* + 1. K3 - Řízení virtuálních desktopů

Implementované řešení založené na produktech společnosti Imprivata umožní zaměstnancům KKN snadné sdílení koncové pracovní stanice a rychlý přesun mezi různými pracovišti, při zachování jeho nezaměnitelné identity.

Řešení bude navrženo a implementováno jako vysoce dostupné a integrováno na sávající řešení zadavatele s odolností vůči výpadku jednoho prvku, a to jak na úrovni fyzických HW prvků, tak na úrovni virtuálních strojů.

Přístup k vzdálené pracovní ploše bude přístupovým bodem, který bude odolný vůči výpadku párového prvku a který bude distribuovat uživatelská sezení mezi jednotlivé hostitelské servery vzdálené pracovní plochy. Informace o uživatelských sezeních budou uchovávány v databázi.

Bude a zavedeno komplexní řešení jednotného přihlašování (Single Sign-On) a silné autentizace.

Tento informační systém pro autentizaci (identifikaci) jednotlivých zaměstnanců umožní rychlé a bezpečné přihlášení k vlastní pracovní ploše na kterémkoliv koncovém zařízení.

Uživatelé budou využívat pro svou identifikaci bezkontaktní kartu, která kromě běžných identifikačních služeb bude umožňovat rychlé a bezpečné přihlášení k pracovní ploše konkrétního uživatele na koncových zařízeních (profil, SSO – Single Sign-On).

Nabízené řešení bude dodáno včetně všech implementačních služeb a potřebného zaškolení obslužného personálu KKN.

* + 1. Implementační kroky

Následující tabulky přehledně shrnují jednotlivé implementační kroky včetně jejich časové souslednosti. Z přehledu je patrné, některé kroky budou vykonávány paralelně a/nebo pro více komodit současně.

|  |  |
| --- | --- |
| **Implementační krok** | **Komodita** |
| Zpracování před-implementační analýzy. Před-implementační analýza bude pokrývat min. následující oblasti:   * + 1. analýzu procesů a aplikací KKN se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí,     2. analýzu požadavků KKN zasílaných informačním systémům s požadavkem na autorizaci a autentizaci,     3. technologický popis stávajících technologií s vazbou na systém správy identit     4. analýzu možností správy výstupních struktur,     5. analýzu evidenčních údajů a logů,     6. návrh životního cyklu identity uživatelů,     7. model organizační struktury,     8. seznam systemizovaných pracovních pozic,     9. přiřazení pracovníků k pracovním pozicím,     10. atributy poskytované personálním systémem v souladu s potřebami obsluhovaných systémů a návrh jejich využití,     11. manažerský souhrn vhodný pro prezentaci výstupů analýzy vedení KKN. | K1 |
| Zpracování před-implementační analýzy. Před-implementační analýza bude pokrývat min. následující oblasti:   * 1. Analýza dokumentů a procesů relevantních pro implementaci požadovaných aplikací - modulů   2. Návrh vhodných datových struktur, kategorií a metadat, přístupových oprávnění a rolí včetně skupin,   3. Návrh a realizace vstupních, stavových a výstupnách formulářů a dokumentů požadavků   4. Analýza funkcionalit API HELIOS Green a realizace potřebných datových importů a/nebo dotazů.   5. Návrh vhodných pracovních postupů (workflow).   6. Implementace systému dle provedených návrhů a doporučení výrobce   7. Návrh a realizace konfiguračních změn infrastruktury   8. Návrh a provedení akceptačních testů | K2 |
| Zpracování před-implementační analýzy. Před-implementační analýza bude pokrývat min. následující oblasti:   * 1. Návrh systému pro vícefaktorové ověřování uživatelů včetně vhodných politik   2. Návrh začlenění vícefaktorového ověřování uživatelů do prostředí aplikační virtualizace – k dispozici bude vícefaktorové i běžné (jméno, heslo) ověřování   3. Návrh vhodných aplikačních sad pro vybrané uživatelské role a způsob jejich spuštění a automatického přihlašování   4. Návrh způsobu realizace požadovaných scénářů "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi"   5. Implementace systému dle provedených návrhů a doporučení výrobce   6. Návrh a provedení akceptačních testů | K3 |
| Předimplementační workshop | K1 |
| Analýza procesů a aplikací KKN se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí. | K1 |
| Technologický popis stávajících technologií s vazbou na systém správy identit. | K1 |
| Analýza možností správy výstupních struktur. | K1 |
| Analýza evidenčních údajů a logů. | K1 |
| Návrh životního cyklu identity uživatelů. | K1 |
| Model organizační struktury. | K1 |
| Seznam systemizovaných pracovních pozic a přiřazení pracovníků k pracovním pozicím. | K1 |
| Atributy poskytované personálním systémem v souladu s potřebami obsluhovaných systémů a návrh jejich využití. | K1 |
| Manažerský souhrn vhodný pro prezentaci výstupů analýzy vedení KKN. | K1 |
| Zapracování výstupů analýzy | K1 |
| Návrh implementace systému IDM. | K1 |
| Návrh napojení na požadované systémy ze strany KKN. | K1 |
| Návrh a provedení akceptačních testů. | K1 |
| Návrh požadovaných úprav stávajících systémů. | K1 |
| Příprava implementačního balíku IDM. | K1 |
| Provedení nezbytných součinností na straně napojovaných systémů ze strany IDM. | K1 |
| Instalace IDM do prostředí KKN. | K1 |
| Provedení testů systému IDM. | K1 |
| Provedení simulačních synchronizací. | K1 |
| Spuštění řádných pravidelných synchronizací. | K1 |
| Předimplementační workshop | K2 |
| Návrh konfigurační databáze pro zavedení do systému | K2 |
| Návrh vhodného způsobu iniciačního zavedení evidovaného majetku (naplnění databáze) SQL | K2 |
| Analýza životního cyklu požadavků a souvisejících procesů ve vztahu k řešeným oblastem | K2 |
| Návrh Integrace s HELIOS Green pro získávání potřebných údajů | K2 |
| Návrh vhodných pracovních postupů (workflow) pro řešení požadavků | K2 |
| Implementace systému dle provedených návrhů a doporučení výrobce | K2 |
| Přiřazeny role jednotlivým uživatelům . | K2 |
| Implementace systému bude provedena dle doporučení výrobce | K2 |
| Otestování kompletního životního cyklu | K2 |
| Návrh a provedení akceptačních testů | K2 |
| Předimplementační workshop | K3 |
| Nasazení 2x virtuální appliance a jejich integrace do virtualizačního prostředí zákazníka | K3 |
| Iniciační konfigurace obou appliance, vytvoření nového "Enterprise" (Prostředí) | K3 |
| Provedení aktualizace obou appliance na poslední verzi | K3 |
| Iniciační nastavení Enterprise - zalicencování, nastavení logování, certifikáty, zálohování apod. | K3 |
| Integrace OneSign s Active Directory a iniciační synchronizace uživatelů | K3 |
| Vytvoření výchozích politik pro uživatele a koncové stanice, vytvoření pravidel pro automatické aplikování politik | K3 |
| Integrace OneSign s MS Remote Desktop Access | K3 |
| Instalace Imprivata OneSign agentů na koncová zařízení a do virtuálních strojů | K3 |
| Vytvoření Single Sign-On profilů pro dispečerské aplikace | K3 |
| Ověření aplikování politik na koncové stanice a uživatele, ověření funkčnosti Imprivata OneSign agentů a celého prostředí | K3 |
| Ladění přihlašovacího workflow uživatele, ladění rychlého střídání pracovišť uživateli, ladění Single Sign-On do aplikací, ladění případných dalších procesů. | K3 |
| Poimplementační zazálohování celého prostředí, export konfigurace. | K3 |
| Celková revize provedení, dokončovací práce – kontrola zálohování, optimalizace konfigurací | K1-K3 |
| Zkušební provoz, technická podpora v jeho průběhu | K1-K3 |
| Zpracování provozní dokumentace | K1-K3 |
| Zpracování materiálů pro školení | K1-K3 |
| Školení administrátorů | K1-K3 |
| Akceptační testy | K1-K3 |
| Předání do plného rutinního provozu | K1-K3 |
| Poskytování systémové podpory | K1-K3 |

* 1. Součinnosti
     1. Časová náročnost

Nezbytnou podmínkou úspěšné implementace je kvalitní součinnost specialistů, ale i uživatelů zadavatele. Uchazeč si je vědom velkého časového vytížení zaměstnanců zadavatele, proto omezí požadavky na součinnost na nezbytné minimum. Vzhledem k rozsahu projektu předpokládáme následující časové nároky na činnosti, u nichž je nezbytná součinnost (účast) specialistů zadavatele:

• Projektové schůzky, úvodní workshopy – 16 hod

• Připomínkování, schvalování dokumentace – 8 hod

• Asistence při instalaci a testování aplikací – 12 hod

• Akceptační testy – 8 hod

• Školení – 16 hod

• Jiná součinnost (zajištění přístupů, poskytnutí dokumentací apod.) – 4 hod

* + 1. Odborná náročnost

V rámci požadované součinnosti nebudou po zaměstnancích – zejména administrátorech – zadavatele požadovány žádné speciální odborné znalosti či dovednosti nad rámec aktuálně rutinně prováděných činností. Klíčovým přínosem administrátorů pro úspěch projektu je celková znalost prostředí zadavatele, způsobů využívání IT technologií, pracovních zvyklostí uživatelů a technických omezení či slabých míst stávajících technologií a řešení.

* 1. Podklady pro hodnocení

Doplňující informace implementačního postupu, členěné dle bodů pro hodnocení kvality implementačního postupu.

* + 1. Popis implementačního procesu

**Metodika implementace zohledňuje potřeby zadavatele v plném rozsahu, obsahuje detailní a jednoznačný popis postupu uchazeče při realizaci předmětu plnění, zcela pokrývající požadavky ZD.**

**50 bodů**

Uchazeč předkládá detailně propracovaný, zcela vyhovující a jednoznačný postup realizace předmětu plnění. Navržený postup v míře a detailu danými vstupními informacemi popisuje jednoznačný postup realizace předmětu plnění v členění po jednotlivých krocích, ze kterých je patrné naplnění zadání. Uchazeč v nabídce předkládá podrobný popis implementačního procesu tak, aby splnil technická kritéria a obecně platné technické předpisy a normy. V rámci popisů procesů a služeb uchazeč specifikuje i procesy nad rámec běžného uživatelského komfortu. Splněním technických kritérií uchazeč rozumí zprovoznění a nastavení dodaných technologií jednak v souladu s naplněním požadavků zadavatele na provedení služby či konkrétní funkčnost a jednak v souladu s doporučenými postupy výrobců, které de facto reprezentují technické předpisy pro používání dodaných technologií. Dodržování obecných technických norem a předpisů (typicky Vyhláška č. 50/1978 Sb a další) je dáno certifikacemi o zavedení systém řízení jakosti uchazeče a jeho subdodavatelů dle ISO 9001 a dalších – <http://www.autocont.cz/o-spolecnosti/rizeni-kvality>

* + 1. Kompatibilita se současným prostředím

**Metodika implementace zohledňuje stávající prostředí zadavatele v plném rozsahu, z metodiky jednoznačně vyplývá, že implementované řešení je plně kompatibilní se současným prostředím zadavatele.**

**20 bodů**

Uchazeč v nabídce prokazuje, že implementované řešení je plně kompatibilní se současným prostředím zadavatele. Technická kompatibilita navrženého řešení je splněna ve všech bodech podstatných pro bezproblémovou funkčnost řešení:

* softwarové produkty K2 a K3 navrhujeme jako rozšíření stávajících řešení zadavatele ALVAO a Imprivata
* Nabízené řešení K1 a K2 podporuje SQL
* Nabízené řešení komodity K3 je možné integrovat do stávajících klientů MS Outlook

## Optimalizace zachování a využití stávajících investic

**Metodika implementace přesvědčivě demonstruje zohlednění stávajícího prostředí zadavatele v návrhu technického řešení v plném rozsahu, z metodiky jednoznačně vyplývá, že implementované řešení je plně kompatibilní se současným prostředím zadavatele. Metodika implementace zároveň jasně definuje kritické body pro zajištění kompatibility se stávajícím prostředím zadavatele a přístup k nim a z popisu je patrné, že dodavatel disponuje know-how v oblasti jejich řešení.**

**10 bodů**

Uchazeč v nabídce prokazuje, že navržený postup implementace spolu s nabízenými produkty velmi úzce navazuje na současný stav (využívá maximum dostupných prostředků a technologií) a výrazným způsobem rozšiřuje a vylepšuje vlastnosti řešení tak, aby byla eliminována slabá místa současného stavu a současně byly doplněny funkce a vlastnosti odpovídají současným trendům a požadavkům v ICT. Nové systémy budou začleněny do stávajícího ICT prostředí a zvýší rozsah i úroveň poskytovaných ICT služeb a zabezpečení.

* + 1. Uplatnění doporučených postupů

**Metodika implementace popisuje velmi propracovaně a synopticky (tedy ve vzájemné provázanosti) systém doporučených postupů výrobců dodávaných zařízení a tzv. best practice (nejlepších praktik), které bude uplatňovat při realizaci zakázky. Z popisu je evidentní vysoký stupeň znalosti doporučených postupů a best practices a patrné know-how při jejich praktické aplikaci.**

**10 bodů**

Uchazeč v nabídce prokazuje znalost a uplatnění doporučených postupů výrobců a tzv. best practice (nejlepších praktik). Navržené implementační kroky prokazují znalosti doporučených postupů např. instalační postup terminálové farmy RDS (testování aplikací, sizing serverů, instalace) apod. Kompletní soupis použitých doporučených postupů je dle mínění uchazeče nad rámec určení tohoto dokumentu (jde o desítky), výše v textu jsou uvedeny ty nejdůležitější odkazy. Uplatnění nejlepších praktik je patrné z navržených implementačních kroků.

* + 1. Minimalizace kapacitní náročnosti

**Metodika implementace zohledňuje potřeby zadavatele v plném rozsahu, postup implementace minimalizuje kapacitní náročnost na zadavatele (zajištění součinnosti, tj. zajištění personálních kapacit zadavatele) při realizaci předmětu plnění.**

**10 bodů**

Uchazeč minimalizuje kapacitní náročnost na zadavatele v oblasti administrativní a organizační (viz. Řízení implementace) i v oblasti časové a odborné náročnosti (viz. Součinnosti)

* + 1. Hodnocené parametry technického řešení

**Uchazečem nabízené řešení zcela splňuje všechny hodnocené parametry technického řešení.**

**3 body**

|  |  |  |
| --- | --- | --- |
| **Hodnocené parametry** | | |
| **Parametr** | **Popis** | **Uchazeč popíše způsob naplnění tohoto hodnoceného parametru včetně značkové specifikace nabízených dodávek** |
| **Snížení nároků na správu systému** | | |
| 1 | Z důvodu zachování jednotné datové základny, její správy a zálohování budou systémy komodit K1 a K2 využívat pro ukládání dat databázový server MS SQL server | Systémy komodit K1 a K2 budou využívat pro ukládání dat databázový server MS SQL server |
| **Uživatelské přívětivost a snížení nároků na správu** | | |
| 2 | Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K1 bude v českém jazyce | Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K1 bude v českém jazyce |
| **Integrace s MS Outlook - Komodita K2** | | |
| 3 | Systém bude integrován s MS Outlook (2010 a vyšší). Integrací se rozumí rozšíření prvků MS Outlook (ribbon – pás karet, formuláře a jejich ovládací prvky) o možnost správy požadavků přímo v prostředí MS Outlook. | Systém Alvao ServiceDesk je plně integrován s prostředím Microsoft Outlouk pomocí speciálního pluginu, který rozšiřuje ovládací prvky MS Outlook o možnost plné správy požadavků – viz. https://www.alvao.cz/produkty/service-desk/ - „Pracujte přímo z Outlooku“ |

* 1. Shrnutí

Celkově z popisu implementačního postupu vyplývá, že nabízený postup implementace povede k úspěšnému splnění předmětu plnění a naplnění veškerých požadavků zadavatele.