S170/2021/0054/01

Smlouva o dodávce licencí a implementačních služeb systémů IDM a PAM

uzavřená ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění
(dále jen „občanský zákoník")

Níže uvedeného dne, měsíce a roku uzavřeli:

1. Městská část Praha 2
se sídlem: nám. Míru 600/20, 120 00 Praha 2
IČO: 00063461
DIČ: CZ00063461
zastoupen: Bc. Janem Kolářem, místostarostou

(dále jen „**Objednatel**" na straně jedné)

a

2. TOTAL SERVICE a.s.
se sídlem: U Uranie 954/18, Holešovice, 170 00 Praha 7
[redacted]
IČO: 256 18 067
DIČ: CZ25618067
zastoupen: Jiřím Chovancem, členem představenstva
ID datové schránky: zcq7wsh
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddílu B pod spisovou značkou 23580
(dále jen **„Poskytovatel"** na straně druhé)

(Objednatel a Poskytovatel dále též označováni jako „**smluvní strany**" nebo „**účastníci smlouvy**")

tuto smlouvu (dále jen „Smlouva")

1. ÚVODNÍ USTANOVENÍ

1.1 Tato Smlouva je uzavírána na základě výsledků zadávacího řízení na veřejnou zakázku malého rozsahu s názvem „Pořízení a implementace systému pro správu digitálních identit (IDM) a privilegovaných přístupů (PAM)". Poskytovatel je seznámen s veškerými zadávacími podmínkami předmětné veřejné zakázky, na základě, které je uzavřena tato smlouva a považuje je za závazné.

1.2 Poskytovatel potvrzuje, že se v plném rozsahu seznámil s rozsahem a povahou služeb a dalších plnění, které bude plnit na základě této Smlouvy, že jsou mu známy jejich veškeré technické, kvalitativní a jiné podmínky a že disponuje takovými kapacitami a odbornými znalostmi, které jsou k plnění nezbytné. Výslovně potvrzuje, že prověřil veškeré podklady a pokyny Objednatele, které obdržel do dne uzavření této Smlouvy i pokyny, které jsou obsaženy v zadávacích podmínkách, které Objednatel stanovil pro zadání této Smlouvy, že je shledal vhodnými, že sjednaná cena a způsob plnění obsahuje a zohledňuje všechny výše uvedené podmínky a okolnosti.

2. PŘEDMĚT SMLOUVY

Předmětem Smlouvy je závazek Poskytovatele:

a) dodat licence systému pro správu digitálních identit (IDM), který bude spravovat a aktualizovat minimálně 300 aktivních digitálních identit a neomezený počet neaktivních digitálních identit. Digitálními identitami se rozumí:

   - digitální identita uživatele (kmenový zaměstnanec Objednatele) interních informačních systémů Objednatele a externích informačních systémů, se kterými uživatel pracuje
   - digitální identita externího pracovníka, který zajišťuje služby technické podpory interních informačních systémů Objednatele a jeho provozní ICT infrastruktury
   - digitální identita ostatních uživatelů informačních systémů Objednatele (uživatelé s oprávněným zájmem přístupu k datové základně Objednatele),

b) dodat technickou podporu výrobce sytému IDM na dobu minimálně 24 měsíců,

c) dodat licence systému pro správu privilegovaných přístupů (PAM), který bude zabezpečovat, řídit a monitorovat přístup až 30 uživatelů ke kritickým datům, systémům a zdrojům Objednatele,

d) dodat technickou podporu výrobce sytému PAM na dobu minimálně 24 měsíců,

e) dodat služby implementace a nastavení IDM a PAM v prostředí Objednatele včetně integrace na služby Microsoft AD a personálního aplikačního systému Objednatele, tj. aplikace Datacentrum 2.

   Zejména se jedná o tyto služby:
   - předprojektová analýza implementace IDM a PAM
   - projektové vedení implementace IDM a PAM
   - dodání administrátorské a uživatelské dokumentace
   - asistence při zkušebním provozu v délce min. 2 měsíce
   - školení administrátorů v nutném rozsahu pro základní správu systému IDM a PAM

3. ZPŮSOB POSKYTOVÁNÍ SLUŽEB

3.1 Poskytovatel se zavazuje při poskytování služeb provozní implementace IDM a PAM vycházet ze stávajícího stavu infrastruktury ICT Objednatele, který je ve stavu aktuálním ke dni uzavření této Smlouvy.

3.2 Poskytovatel zahájí plnění předmětu Smlouvy dle odstavce 2. této Smlouvy nejpozději do 14 dnů ode dne nabytí účinnosti této Smlouvy.

3.3 Poskytovatel je povinen upozornit Objednatele na rizika spojená s realizací provozních implementačních služeb systému IDM a PAM dle odstavce 2. bod e) této Smlouvy. Pokud by plnění Objednatelem požadovaných provozních implementačních služeb vedlo ke zhoršení výkonu ICT infrastruktury Objednatele či vzniku poruch a škod, je Poskytovatel povinen na tuto skutečnost Objednatele předem upozornit. Pokud Objednatel i přes upozornění Poskytovatele provedené dle tohoto článku Smlouvy trvá na plnění stanoveném v požadavku, Poskytovatel neodpovídá za škody vzniklé plněním provozních implementačních služeb dle požadavku, ledaže překročil pokyny vydané Objednatelem.

3.4 Veškeré vady zjištěné v průběhu nebo po realizaci implementačních služeb je Objednatel povinen oznamovat Poskytovateli. V případě, že v průběhu realizace implementace nebo po dokončení její realizace Objednatel zjistí dvě a více vad ICT infrastruktury Objednatele způsobené implementací, je oprávněn implementaci jednostranně ukončit. Poskytovatel je povinen opravit zjištěné vady v termínech dle dohody a informovat Objednatele o možnosti pokračování v poskytování implementačních služeb.

3.5 O dokončení implementačních služeb (včetně dokončení integrace na služby Microsoft AD a personální systém Objednatele Datacentrum 2) bude vyhotoven zápis, který bude podepsán oprávněnými osobami obou stran.

3.6 Po dokončení implementačních služeb zahájí Objednatel zkušební provoz systémů IDM a PAM. Během zkušebního provozu budou pověřenými pracovníky vyzkoušeny požadované funkcionality (viz příloha č. 1 této Smlouvy) systémů IDM a PAM. Zkušební provoz bude probíhat minimálně 2 měsíce.

3.7 O ukončení zkušebního provozu (včetně otestování integrace na služby Microsoft AD a personální systém Objednatele Datacentrum 2) bude vyhotoven zápis, který bude podepsán oprávněnými osobami obou stran.

3.8 Objednatel se zavazuje poskytnout potřebnou součinnost a zdroje pro otestování IDM a PAM během trvání zkušebního provozu.

3.9 Poskytovatel se zavazuje spolupracovat s třetími stranami, poskytujícími služby v podpoře a správě HW a SW, týkající se infrastruktury ICT Objednatele a interních nebo externích informačních systémů a služby Microsoft AD.

4. TERMÍN A MÍSTO PLNĚNÍ

4.1 Poskytovatel se zavazuje zahájit plnění dle této Smlouvy nejpozději do 14 dnů ode dne účinnosti této smlouvy a postupovat podle harmonogramu viz příloha č. 1. Část III. „Harmonogram, plán implementace IDM+PAM a odstávek"

4.2 Místem plnění jsou určené prostory Objednatele, tzn. budova ÚMČ Praha 2, nám. Míru 20/600, 120 39 Praha 2

5. CENA A PLATEBNÍ PODMÍNKY

5.1 Objednatel se zavazuje uhradit Poskytovateli:

cenu celkem ve výši 1.846.000, - Kč bez DPH

výše DPH v %. 21 tj. výše DPH v Kč 387.660, - Kč

cenu celkem ve výši 2.233.660, - Kč včetně DPH

Celková cena bude uhrazena ve třech splátkách takto:

Splátka Akceptační milník	Akce	Výše splátky v % z celkové ceny v Kč bez DPH
1.	Akceptovaná dodávka licencí, technické podpory výrobce na 24 měsíců a instalace systémů IDM a PAM v prostředí Objednatele	50
2.	Akceptovaná integrace IDM na MS AD a personální system Datacentrum 2 Objednatele, akceptovaná dodávka administrátorské a uživatelské aplikace a školení administrátorů	35
3.	Akceptovaná dodávka asistence při zkušebním provozu po dobu min. 2 měsíců	15

5.2 Cena za plnění předmětu dle této smlouvy je konečná a celková a může být měněna pouze v souvislosti se změnou sazeb DPH či jiných daňových předpisů majících vliv na cenu za poskytnutí plnění. Rozhodným dnem pro změnu ceny za poskytnutí plnění z důvodu zákonné změny sazby DPH je den zdanitelného plnění.

5.3 V celkové ceně jsou zahrnuty veškeré náklady prodávajícího nezbytné pro řádnou a včasnou dodávku předmětu plnění dle této smlouvy, tedy doprava, veškeré práce, dodávky, služby, poplatky, výkony a další činnosti nutné pro řádné splnění předmětu této smlouvy.

5.4 Cena za poskytnutí plnění bude kupujícím uhrazena v českých korunách na základě prodávajícím řádně a oprávněně vystaveného účetního a daňového dokladu (dále jen „faktura"). Cena za poskytnutí plnění bude uhrazena na základě faktury. Lhůta splatnosti faktury se sjednává na 30 dnů ode dne jejího

prokazatelného doručení kupujícímu. V případě prodlení kupujícího s úhradou faktury se kupující zavazuje uhradit prodávajícímu úrok z prodlení ve výši 0,001 % z příslušné dlužné částky za každý den prodlení.

5.5 Faktura – daňový doklad bude vystavena v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. Faktura bude Poskytovatelem odeslána na adresu Objednatele a bude mít, kromě zákonem stanovených údajů, zejména tyto náležitosti:

a) datum splatnosti;

b) číslo Smlouvy,

c) Výkaz poskytovaných Služeb;

d) vyčíslení slev z ceny;

e) IČ a DIČ Poskytovatele a Objednatele

5.6 V případě, že zaslaná faktura nebude mít náležitosti daňového dokladu nebo na ní nebudou uvedeny údaje specifikované v čl. 5.5 této Smlouvy, nebo bude neúplná a nesprávná, je Objednatel oprávněn tuto fakturu ve lhůtě splatnosti Poskytovateli vrátit k opravě či doplnění. V takovém případě lhůta splatnosti faktury běží až od okamžiku doručení opravené faktury Objednateli.

5.7 Platby peněžitých částek se provádí bankovním převodem na účet druhé smluvní strany uvedený ve faktuře. Peněžitá částka se považuje za zaplacenou okamžikem jejího odepsání z účtu odesílatele ve prospěch účtu příjemce.

6. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

6.1 Smluvní strany se zavazují informovat bez zbytečného odkladu druhou smluvní stranu o veškerých skutečnostech, které jsou významné pro plnění závazků smluvních stran.

6.2 Poskytovatel je povinen realizovat předmět této Smlouvy řádně, pečlivě a v souladu s obecně závaznými právními předpisy. Dostane-li se Poskytovatel do prodlení s plněním dle této Smlouvy bez zavinění Objednatele či v důsledku okolností vylučujících odpovědnost za škodu po dobu delší než pět (5) dnů, je Objednatel oprávněn zajistit plnění dle této Smlouvy po dobu prodlení Poskytovatele jinou osobou; v takovém případě nese náklady spojené s náhradním plněním Poskytovatel.

6.3 Poskytovatel je povinen dodržovat veškeré interní předpisy Objednatele, se kterými byl seznámen. Poskytovatel je povinen zajistit, aby všechny osoby podílející se na poskytování plnění dle této Smlouvy tyto předpisy dodržovaly.

6.4 Poskytovatel je povinen upozorňovat Objednatele na případnou nevhodnost pokynů Objednatele.

6.5 V případě, že dojde k výběru nového subjektu odlišného od Poskytovatele, který bude poskytovat Objednateli služby obdobné implementačním službám dle této Smlouvy, nebo Objednatel zahájí nebo bude zvažovat výběr takovéhoto poskytovatele, zavazuje se Poskytovatel dle pokynů Objednatele poskytnout veškerou potřebnou součinnost, dokumentaci a informace a účastnit se jednání s Objednatelem a novým poskytovatelem za účelem plynulého a řádného převedení migračních služeb či jejich příslušné části na nového poskytovatele a poskytnout potřebnou součinnost až do úplného převedení.

6.6 Poskytovatel je oprávněn k poskytování plnění dle této Smlouvy využít subdodavatele. Při poskytování plnění dle této Smlouvy prostřednictvím subdodavatele odpovídá Poskytovatel, jako by toto plnění poskytoval sám.

6.7 Poskytovatel odpovídá za bezpečnost svých pracovníků. Před zahájením činnosti budou všichni pracovníci proškoleni o dodržování bezpečnosti práce odpovídající místním bezpečnostním pravidlům, a to v součinnosti s odborným specialistou Objednatele.

6.8 Poskytovatel je povinen do 5 dnů ode dne nabytí účinnosti této Smlouvy předložit Objednateli seznam pracovníků, kteří se budou podílet na poskytování plnění dle této Smlouvy, a tento seznam průběžně aktualizovat.

6.9 Poskytovatel se zavazuje, že poskytování plnění dle této Smlouvy neomezí současný provoz informačních systémů Objednatele a neohrozí bezpečnost v prostorách Objednatele.

6.10 Poskytovatel je povinen uzavřít pojistnou smlouvu pro případ odpovědnosti za škodu způsobenou třetí osobě v souvislosti s plněním předmětu této Smlouvy v rozsahu min.2.000.000,- Kč, a to po celou dobu trvání této Smlouvy. Existenci pojistné smlouvy je Poskytovatel povinen prokázat Objednateli ke dni účinnosti této Smlouvy a neprodleně Objednateli písemně oznámit případné změny v těchto skutečnostech, jinak Poskytovatel odpovídá za případnou škodu, která nesplněním této povinnosti vznikne. Na požádání je Poskytovatel povinen Objednateli takovou pojistnou smlouvu bezodkladně předložit.

6.11 Objednatel se touto Smlouvou zavazuje poskytnout Poskytovateli veškerou součinnost nezbytnou pro poskytování plnění dle této Smlouvy,

7. LICENČNÍ UJEDNÁNÍ

7.1 Bude-li součástí Služeb nebo výsledkem činnosti Poskytovatele prováděné dle této Smlouvy autorské dílo podle zákona č. 121/2001 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorské dílo"), nabývá Objednatel dnem poskytnutí autorského díla Objednateli k užívání nevýhradní právo užít takovéto autorské dílo všemi způsoby nezbytnými k naplnění účelu vyplývajícímu z této Smlouvy, a to po celou dobu trvání autorského práva k autorskému dílu bez omezení rozsahu množstevního, technologického, teritoriálního (dále jen ,,Licence"). Součástí Licence je rovněž neomezené právo Objednatele poskytnout třetím osobám podlicenci k užití autorského díla v rozsahu shodném s rozsahem Licence, souhlas Poskytovatele k postoupení Licence na třetí osoby a souhlas Poskytovatele udělený Objednateli k provedení jakýchkoliv změn nebo modifikací autorského díla, a to i prostřednictvím třetích osob. Licence se automaticky vztahuje i na všechny nové verze, aktualizované verze, i na úpravy a překlady autorského díla, dodané Poskytovatelem. Poskytovatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorskému dílu a že má souhlas autorů k uzavření těchto licenčních ujednání a že toto prohlášení zahrnuje i taková práva autorů, která by vytvořením autorského díla teprve vznikla.

7.2 Poskytovatel je povinen postupovat tak, aby údělem Licence k autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci zabezpečil, a to bez újmy na právech třetích osob. Nebude-li výjimečně možné po Poskytovateli spravedlivě požadovat udělení Licence v rozsahu dle čl. 8.1 této Smlouvy, zejména proto, že se jedná o tzv. standardní počítačové programy, je Poskytovatel povinen na to písemně Objednatele upozornit spolu s náležitým odůvodněním a poskytnout Objednateli nebo zajistit pro Objednatele poskytnutí licence či podlicence v nejširším možném rozsahu. Postup dle předchozí věty je možný jen s výslovným písemným souhlasem Objednatele, přičemž se Objednatel zavazuje, že tento souhlas neodmítne poskytnout bez vážného důvodu.

7.3 Bude-li autorské dílo vytvořeno činností Poskytovatele, smluvní strany činí nesporným, že jakékoliv takovéto autorské dílo vzniklo z podnětu a pod vedením Objednatele.

7.4 Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Poskytovatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Poskytovatelem Objednateli.

7.5 Odměna za poskytnutí, zprostředkování nebo postoupení Licence k autorskému dílu je zahrnuta v ceně Služeb, při jejichž poskytnutí došlo k vytvoření autorského díla.

8. ODPOVĚDNOST ZA ŠKODU A SMLUVNÍ POKUTY, SLEVA Z CENY, ÚROK Z PRODLENÍ

8.1 Smluvní strany nesou odpovědnost za způsobenou škodu dle příslušných právních předpisů a dle této Smlouvy.

8.2 Smluvní strana, která poruší svou povinnost plynoucí z této smlouvy nebo z obecně závazných právních předpisů, je povinna nahradit škodu tím způsobenou druhé straně, ledaže prokáže, že porušení povinnosti bylo způsobeno okolnostmi vylučujícími odpovědnost. Nárok na náhradu škody není dotčen zaplacením jakékoliv smluvní pokuty dle této smlouvy.

8.3 Poskytovatel se zavazuje uhradit Objednateli či orgánu veřejné moci veškeré finanční částky, které budou poskytovateli ve správním, soudním či jiném obdobném řízení uloženy jako pokuty či jiné majetkoprávní sankce za poskytovatelem způsobené porušení právních povinností.

8.4 Žádná ze smluvních stran není odpovědná za škodu nebo prodlení způsobené okolnostmi vylučujícími odpovědnost ve smyslu zákona č. 89/2012 Sb., občanského zákoníku. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost a bránící řádnému plnění smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

8.5 Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Poskytovatel je povinen upozornit Objednatele na rizika vzniku škod a včas a řádně dle svých možností provést taková opatření, která riziko vzniku škod zcela vyloučí nebo sníží.

8.6 V případě prodlení Poskytovatele s dodržením sjednaného termínu zahájení poskytnutí plnění dle této Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 3000,- Kč, a to za každý započatý den a případ prodlení.

8.7 V případě, že Poskytovatel poruší některou ze svých povinností stanovenou mu čl. 9. této Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 5.000,- Kč za každé jednotlivé porušení.

8.8 Smluvní pokuty dle této Smlouvy jsou splatné do 15 dnů od doručení výzvy Objednatele k její úhradě Poskytovateli. Objednatel si vyhrazuje právo na určení způsobu úhrady smluvní pokuty, a to včetně formy zápočtu proti kterékoliv splatné pohledávce Poskytovatele vůči Objednateli, Objednatel je tedy oprávněn započítat smluvní pokuty proti Poskytovatelem fakturovaným částkám za plnění a Poskytovateli bude tedy uhrazena fakturovaná částka snížená o příslušnou smluvní pokutu.

8.9 Zaplacením smluvní pokuty dle této Smlouvy není dotčena povinnost k náhradě škody způsobené porušením příslušné povinnosti v plné výši.

8.10 V případě prodlení Objednatele s placením daňového dokladu ve sjednané lhůtě splatnosti je Poskytovatel oprávněn účtovat Objednateli úrok z prodlení ve výši dvou setin procenta (0,05 %) z dlužné částky za každý i započatý den prodlení.

8.11 V případě prodlení Poskytovatele s úhradou platby, na níž vznikl Objednateli nárok, a to zejména pokud jde o smluvní pokuty, je Poskytovatel povinen Objednateli uhradit úrok z prodlení ve výši dvou setin procenta (0,05 %) z dlužné částky za každý i započatý den prodlení.

8.12 Za porušení povinnosti Poskytovatele udržovat v platnosti pojištění odpovědnosti dle článku 6 odst. 6.10 této smlouvy bude Objednatel oprávněn účtovat Poskytovateli smluvní pokutu ve výši 50.000,- Kč za každý zjištěný případ.

9. OCHRANA DŮVĚRNÝCH INFORMACÍ

9.1 Smluvní strany jsou si vědomy toho, že v rámci plnění Smlouvy:

- si mohou vzájemně úmyslně nebo i opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „důvěrné informace"),
- mohou jejich zaměstnanci nebo třetí osoby získat vědomou činností druhé Smluvní strany nebo i jejím opominutím či jinak přístup k důvěrným informacím druhé Smluvní strany.

9.2 Předávající strana zůstává výlučným nositelem práv k veškerým důvěrným informacím a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace, zejména bude o nich zachovávat mlčenlivost a zajistí, aby je ve stejném

rozsahu zachovávaly i jiné osoby, kterým je poskytne v souladu s touto Smlouvou. S výjimkou plnění této Smlouvy se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohla být tato Smlouva splněna. V případě plnění této Smlouvy se smluvní strany zavazují činit tak vždy jen v nezbytně nutném rozsahu.

9.3 Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné implicitně všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství, tj. například ale nejenom popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu, nebo jejichž zveřejnění předávající strana výslovně zakázala. Tímto ustanovením nejsou dotčena práva a povinnosti smluvních stran dle čl. 8 této Smlouvy.

9.4 Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivost a povinnost chránit důvěrné informace vyplývající z této smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající z nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „Nařízení GDPR"). Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této smlouvy. Poskytovatel je povinen po celou dobu plnění této smlouvy splňovat veškeré podmínky dle Nařízení GDPR.

9.5 Pokud jsou důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.

9.6 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímající strana,
- měla přijímající strana legálně k dispozici před uzavřením Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací, nebo pokud nejsou chráněny ze zákona,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,
- po podpisu Smlouvy poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je nositelem práv k těmto informacím.

9.7 V případě vzniku mimořádné události, havárie, škody na majetku, zdraví osob apod., bude ve vztahu k informování veřejnosti a k médiím vystupovat vždy Objednatel. Poskytovatel není oprávněn sdělovat zástupcům médií a veřejnosti jakékoli informace, týkající se událostí uvedených v předchozí větě.

9.8 Povinnost mlčenlivosti trvá bez ohledu na ukončení účinnosti této smlouvy.

9.9. Ujednání o ochraně a zpracování osobních údajů tvoří Přílohu č. 2 této smlouvy. Je-li příloha č. 2 této smlouvy v rozporu s Nařízením GDPR, je při výkladu práv a povinností rozhodné aktuálně platné a účinné znění Nařízení GDPR.

10. VZÁJEMNÁ KOMUNIKACE SMLUVNÍCH STRAN

10.1 Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob, pověřených zaměstnanců nebo statutárních orgánů, popřípadě členů statutárních orgánů smluvních stran.

10.2 Každá ze smluvních stran jmenuje oprávněnou osobu. Oprávněné osoby budou zastupovat smluvní stranu ve smluvních a obchodních záležitostech souvisejících s plněním této Smlouvy. Není-li stanoveno jinak, nejsou oprávněné osoby oprávněny ke změnám Smlouvy ani jejímu ukončení, ledaže získají speciální plnou moc.

10.3 Každá smluvní strana je oprávněna změnit jí jmenovanou oprávněnou osobu, resp. jejího zástupce, je však povinna na takovou změnu druhou smluvní stranu písemně upozornit. Vůči druhé smluvní straně je změna účinná okamžikem doručení písemného oznámení této smluvní straně.

10.4 Oprávněné osoby:

Oprávněnou osobou na straně Objednatele jsou:

a) ve věcech smluvních:
Ing. Petr Štěpán, vedoucí odboru informatiky, tel. [redacted]
petr.stepan@praha2.cz

b) ve věcech technických: Ing. Petr Štěpán, vedoucí odboru informatiky, tel. [redacted]
petr.stepan@praha2.cz

[redacted]

Oprávněné osobou na straně Poskytovatele jsou:

a) ve věcech smluvních:
Jiří Chovanec, člen představenstva, tel. [redacted]

b) [redacted]

10.5 Všechny dokumenty mající vztah k plnění této Smlouvy musí být vyhotoveny písemně a podepsány oprávněnými osobami obou smluvních stran.

11. PLATNOST A ÚČINNOST SMLOUVY

11.1 Tato Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v Registru smluv.

11.2 Tuto Smlouvu lze ukončit:

- dohodou smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek,
- odstoupením od Smlouvy v případech uvedených v této Smlouvě
- výpovědí bez udání důvodu

11.3 Objednatel je oprávněn odstoupit od této Smlouvy v těchto případech:

- služby Poskytovatele vykazují v průběhu provádění vady nebo jsou prováděny v rozporu s touto Smlouvou a Poskytovatel ani ve lhůtě dohodnuté s Objednatelem tyto vady neodstraní,
- nedodržení závazných právních, technických, odborných, oborových norem,
- opakované nesplnění sjednaného rozsahu činností dle této smlouvy nebo povinností Poskytovatele dle této smlouvy,
- při porušení ostatních povinností stanovených touto smlouvou v případě, že by takový postup Poskytovatele vedl nepochybně k porušení smlouvy podstatným způsobem,
- Poskytovatel pozbude oprávnění k činnostem, k jejichž provádění je Poskytovatel povinen dle této smlouvy,
- vůči majetku Poskytovatele bude probíhat insolvenční řízení,

- Poskytovatel vstoupí do likvidace,
- Poskytovatel neudržuje pojištění dle čl. 6 odst. 6.10. této smlouvy či existenci tohoto pojištění nedoloží ani v dodatečné lhůtě v délce 5 pracovních dnů,
- Objednateli vznikne opakovaně nárok na zaplacení smluvní pokuty dle čl. 8 této smlouvy

11.4. Za den odstoupení od smlouvy se považuje den, kdy bylo písemné oznámení o odstoupení oprávněné smluvní strany doručeno druhé smluvní straně. Odstoupením od smlouvy nejsou dotčena práva smluvních stran na úhradu smluvní pokuty a na náhradu škody.

11.5. Odstoupení od smlouvy musí být učiněno písemným oznámením o odstoupení od této smlouvy druhé straně, účinky odstoupení nastávají dnem doručení oznámení druhé straně. V pochybnostech se má za to, že odstoupení bylo doručeno do 10 dnů od jeho odeslání v poštovní zásilce s dodejkou, resp. do 10 dnů od jeho odeslání prostřednictvím informačního systému datových schránek.

11.6. Shora uvedené dokumenty se vždy doručují druhé smluvní straně, a to některým ze způsobů dále uvedených:

- Osobně oproti potvrzení o převzetí.
- Doporučeným dopisem či jinou formou na adresu objednatele nebo poskytovatele uvedenou v záhlaví této smlouvy. Pokud v průběhu plnění této smlouvy dojde ke změně adresy některé ze smluvních stran, je tato smluvní strana povinna neprodleně písemně informovat druhou smluvní stranu o této změně. Odeslaná zásilka se má za doručenou desátý den po jejím odeslání. Nevyzvedne-li si adresát zásilku či jinak vědomě zmaří její doručení, platí, že zásilka řádně došla.
- Prostřednictvím datové schránky. V tomto případě se dokumenty považují za doručené okamžikem, kdy odesílatel obdrží od příslušného technického zařízení potvrzení o úspěšném odeslání nebo potvrzení o doručení.

12. ŘEŠENÍ SPORŮ

12.1 Veškerá vzájemná práva a povinnosti Poskytovatele a Objednatele vyplývající z této Smlouvy se budou řídit právem České republiky. Veškeré spory, které vzniknou z uzavřených smluv nebo v souvislosti s nimi a které se nepodaří vyřešit přednostně smírnou cestou, budou rozhodovány obecnými soudy.

13. ZÁVĚREČNÁ USTANOVENÍ

13.1 Tato Smlouva a právní vztahy vzniklé z této Smlouvy se řídí zejména občanským zákoníkem a dalšími právními předpisy ČR.

13.2 Poskytovatel bere na vědomí, že městská část Praha 2 je na základě ustanovení § 2 odst. 1 a ustanovení § 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, subjektem povinným poskytovat na žádost třetí osoby informace, vztahující se k působnosti městské části Praha 2. Poskytovatel uděluje Objednateli souhlas, aby veškeré informace obsažené v této smlouvě byly poskytnuty třetím osobám na základě jejich žádosti.

13.3 Smluvní strany podpisem této smlouvy potvrzují, že jsou seznámeny s tím, že tato smlouva podléhá povinnosti uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

13.4. Tuto Smlouvu lze měnit, doplňovat nebo rušit pouze písemně, není-li v této Smlouvě uvedeno jinak. V případě změny či doplnění dohodou se vyžaduje písemný dodatek k této Smlouvě.

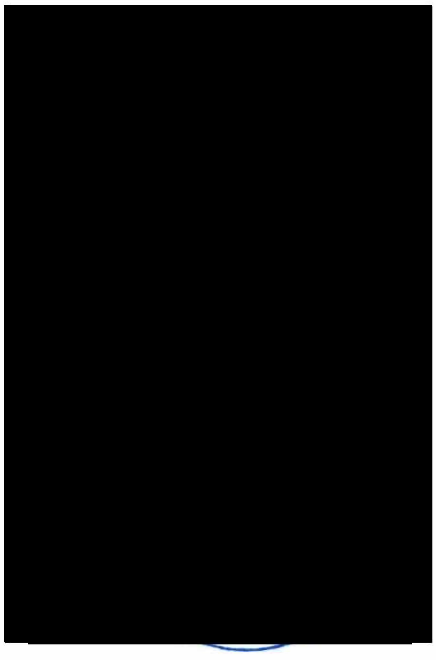
13.5 V případě, že se některé ustanovení této Smlouvy stane neplatným či ne vymahatelným, zůstávají ostatní ustanovení i nadále v platnosti, ledaže právní předpis stanoví jinak. Smluvní strany se zavazují takové neplatné či nevymahatelné ustanovení nahradit jiným, odpovídajícím účelu ustanovení neplatného či nevymahatelného.

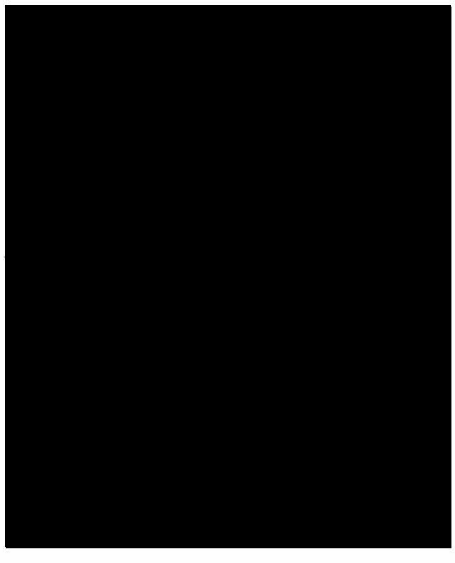
13.6 Tato Smlouva je vyhotovena ve čtyřech (4) stejnopisech, z nichž Objednatel obdrží dva (2) a Poskytovatel dva (2) stejnopisy.

14. PŘÍLOHY

Nedílnou součástí této Smlouvy jsou přílohy:

Příloha č. 1 - Technická specifikace IDM a PAM
Příloha č. 2 – Ujednání o ochraně osobních údajů





Příloha Smlouvy

Příloha č. 1 - Technická specifikace IDM a PAM

Předmět plnění

Předmětem plnění veřejné zakázky je dodávka licencí a implementace systému pro správu digitálních identit (IDM), který bude spravovat a aktualizovat:

- digitální identity interních zaměstnanců využívajících informační systémy Objednatele
- digitální identity externích pracovníků, kteří zajišťují např. služby technické podpory informačních systémů Objednatele a provozní ICT infrastruktury
- digitální identity ostatních uživatelů informačních systémů Objednatele (osoby s oprávněným zájmem přístupu k datové základně Objednatele)

(dále jen uživatelé)

Licence IDM jsou požadovány včetně podpory výrobce na 24 měsíců.

Předmětem plnění veřejné zakázky je dodávka licencí a implementace systému pro správu privilegovaných přístupů (PAM), který bude zabezpečovat, řídit a monitorovat přístup uživatelů ke kritickým datům, systémům a zdrojům Objednatele (administrátoři, správci aplikací atd.)

Licence PAM jsou požadovány včetně podpory výrobce na 24 měsíců.

Předmětem veřejné zakázky je dále soubor služeb, jejichž výstupem je implementace a nastavení IDM a PAM v prostředí Objednatele včetně integrace na vybrané aplikace Objednatele.

Zejména se jedná o tyto služby:

- projektové vedení implementace IDM a PAM
- implementační projekt
- integrace IDM na prostředí Microsoft AD a personální aplikaci Datacentrum 2
- nastavení a metodická podpora pro PAM v prostředí Objednatele
- dodání administrátorské a uživatelské dokumentace k IDM a PAM a jejich implementace v prostředí Objednatele
- technická a metodická asistence při zkušebním provozu IDM a PAM (minimálně po dobu 2 měsíců)
- školení administrátorů IDM a PAM v nutném rozsahu pro základní správu obou systémů

Pokud není výslovně uvedeno jinak, Objednatel disponuje všemi potřebnými licencemi pro provoz svých informačních systémů (IS) a dodávka těchto licencí není předmětem veřejné zakázky.

Popis ICT prostředí Objednatele

Stávající provozní a testovací IT infrastruktura Objednatele využívá virtualizační platformu VMWARE 6.7 v režimu vysoké dostupnosti. Virtualizační platforma je centrálně spravována přes vCenter 6.7. Součásti IT infrastruktury je centrální plně replikované diskové pole s dostatečnou kapacitní rezervou a odpovídajícím výkonem připojené v rámci sítě SAN. Datová struktura pro komunikaci mezi servery a diskovým polem je vybudovaná na technologii fiber channel s využitím SAN switchů a redundantních cest pro případ výpadku.

Obednatel deklaruje používání koncových zařízení uživatelů na platformě Windows 10 (64 bit) a Apple IOS, využívání kancelářského balíku Office 2016 a vyšší, služeb O365 a webových prohlížečů MS Edge, Google Chrome a Firefox v aktuálních verzích.

Objednatel dále provozuje databázové systémy Oracle 12.2.0.1. a MS SQL 2012. V případě, že nabízené systémy IDM nebo PAM jsou implementované na jiném než výše uvedeném databázovém systému, musí Poskytovatel zajistit dodávku všech licencí potřebných pro provoz tohoto databázového systému a jeho instalaci pro minimálně 300 aktivních identit a dlouhodobé uložení historických dat u neomezeného počtu neaktivních identit. Součástí takové dodávky je pak i podpora výrobce databázového systému na dobu min. 5 let.

ČÁST I. Identity Management Systém (IDM)

Obecné požadavky na IDM

- IDM systém bude udržovat a spravovat aktivní identity (uživatelské účty, aplikační oprávnění) a historická data o neaktivních identitách. Spravované identity budou referenčními identitami pro interní i externí informační systémy
- pro správu identit musí být vytvořena jednotná centrální evidence uživatelů včetně jejich uživatelských účtů a oprávnění k integrovaným i neintegrovaným IS MČ Praha 2.
- všechny výše uvedené informace musí být ukládány a udržovány ve vnitřní databázi IDM
- s IDM systémem musí být dodány veškeré potřebné licence pro provoz v infrastruktuře Objednatele (možno využít stávající licence Objednatele, pokud jimi již disponuje
- Poskytovatelem dodané licence musí být trvalé a umožnit udržovat a spravovat min. **300 aktivních identit** a neomezený počet neaktivních identit, neomezený počet integrovaných IS
- dodané licence nesmí Objednatele omezovat v obvyklém používání IDM, tj. počet záznamů v databázi, velikost databáze, počet uživatelů s administrátorskými právy, integrace IS atd.)
- IDM musí umožnit svojí architekturou zvyšování výkonu systému rozložením zátěže na více serverů, a to minimálně oddělením rolí serverů (aplikační server, databázový server)
- IDM musí umožnit nasazení v režimu vysoké dostupnosti (HA cluster)
- IDM musí obsahovat integrovaný registr IS a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby nebo skriptováním
- IDM musí obsahovat integrovanou správu uživatelských rolí, včetně zařazení uživatelů do odpovídající role v konkrétním integrovaném IS
- IDM musí umožnit dodatečné přidávání vlastních atributů k identitám a referenčním objektům (organizační jednotka, aplikační role, systematizované místo atd.), vyplňování jejich obsahu ze zdrojových systémů a jejich následnou publikaci přes rozhraní webových služeb
- IDM musí umožnit správu uživatelských rolí a zařazení uživatelů do odpovídajících rolí v daných IS
- IDM musí umožňovat v intuitivním, přehledném grafickém rozhraní tvořit pravidla pro automatické vytváření uživatelských účtů, přiřazování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.)
- IDM musí umožnit grafické zobrazení identit v přehledné struktuře. Musí být možno vyhledávat jednotlivé identity nebo jejich skupiny, včetně přehledu uživatelů aktuálně pracujících s IDM systémem
- IDM musí umožnit práci přes WEB konzoli s podporou Microsoft Edge, Google Chrome a Mozilla Firefox v aktuálních verzích. WEB konzole bude hlavním rozhraním pro uživatele i administrátory pro přístup k datům, funkcím a administraci včetně integračních úloh IDM
- WEB konzole bude přístupná výhradně přes HTTPS protokol
- WEB konzole musí být implementována s responzivním designem
- IDM musí obsahovat autentizační rozhraní, které umožní IS zprostředkovat autentizační úlohy min. přes následující standardy a protokoly:
    - LDAP (Active Directory)
    - Windows autentizace
    - Radius protokol
    - pomocí certifikátu
    - OpenID
    - Oauth 2.0
    - SAML 2.0 s tím, že IDM musí umožnit plnit roli identity providera a současně roli service providera
- IDM systém musí mít kompletní podporu českého jazyka
- IDM musí obsahovat 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

- IDM musí podporovat správu uživatelských digitálních certifikátů. Data o certifikátech musí být možno do IDM nahrávat přes webové služby
- IDM musí obsahovat nastavení umožňující automatické zneplatnění certifikátů po uplynutí data platnosti
- IDM musí umožnit propojení více uživatelských účtů v různých IS k jedné identitě
- IDM musí obsahovat mechanismus zabraňující hromadným změnám z důvodu případných chybných vstupních dat ze zdrojových systémů (nesmí dojít k hromadným nežádoucím změnám)
- IDM musí podporovat použití filtrů nad atributy objektů. Filtrovat musí být možno dle libovolných atributů identit. Filtry musí být možné ukládat za účelem opakovaného použití
- IDM musí umožnit export zobrazených seznamů do CSV
- IDM musí obsahovat editor vlastních oprávnění a víceúrovňovou správu administrátorských oprávnění. Tato oprávnění musí být definovatelná pro jednotlivé entity a moduly IDM systému (identity, aplikační role, konfigurace notifikací, konfigurace synchronizací s IS, workflow, správa webových služeb atd.). U jednotlivých konkrétních částí IDM bude možnost definovat akce, které může uživatel s přidělenými oprávněními dělat
- IDM musí umožnit k identitám definovat konkrétní atributy včetně zobrazení a editace atributu oprávněným uživatelem IDM, povinnost atributu a pořadí atributu při zobrazení apod.
- IDM musí umožnit zobrazení uživatelské karty, která musí obsahovat osobní údaje uživatele (jméno, příjmení, tituly, osobní číslo, funkční zařazení atd.), aktuální nastavení oprávnění k jednotlivým integrovaným IS. U integrovaných IS musí být zobrazena informace, kdo a kdy o daná oprávnění žádal, kdo a kdy žádaná oprávnění povolil a schválil. Uživatelská karta musí být přehledná a exportovatelná min. do souboru ve formátu PDF
- IDM musí obsahovat přiřazování aplikačních rolí konkrétní identitě, systematizovanému místu, skupině a organizační jednotce včetně data a času konce platnosti přiřazení. Po vypršení data a času platnosti přiřazení bude role systémem IDM automaticky odebrána
- IDM musí umožnit zobrazení přidělených rolí k jednotlivým identitám s rozdělením role navázané na systematizované místo, identitu, organizační jednotku, skupinu. U identity musí IDM systém evidovat souhrnné zobrazení seznamu všech rolí včetně informace o tom, odkud uživatele roli zdědil (skupina, organizační jednotka atd.)
- IDM musí umožnit správu skupin s možností začleňování více skupin do sebe, přiřazovat jednotlivé uživatele do skupin, přiřazovat systematizovaná místa do skupin
- IDM musí obsahovat správu vztahů zastupitelnosti mezi jednotlivými uživateli. IDM musí uživatelům umožnit ve vztahu k organizační struktuře delegovat v případě potřeby svoje role v IDM systému (nemoc, dovolená atd.) s tím, že různé části role mohou být delegovány na různé uživatele
- IDM musí umožnit delegování administrátorských práv
- IDM musí obsahovat webové rozhraní pro uživatele, kde je možné změnit samoobslužně uživatelské heslo a požádat o přidělení jednotlivých aplikačních rolí nebo členství ve skupinách. Role a skupiny budou kategorizovány podle toho, jestli požadavek podléhá schvalovacímu workflow nebo zda může dojít k přiřazení automaticky. Každý požadavek a stav jeho řešení musí být evidován a zpětně dohledatelný v IDM
- IDM musí obsahovat v rámci uživatelského rozhraní konfigurovatelné registrační formuláře pro registraci externích organizací, identit, žádostí o konkrétní aplikační role nebo skupiny. Seznamy rolí a skupin, o které mohou uživatele žádat, musí být v IDM možno specifikovat samostatně pro organizační jednotky
- IDM musí uživatelům umožnit individuální nastavení vlastního rozhraní (zobrazení/skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku pro všechny seznamy samostatně apod.)

Požadavky na synchronizaci

- IDM musí umožnit automatické i ruční spouštění synchronizace s integrovanými systémy a podporovat simulační režim synchronizace
- IDM musí umožnit zobrazení jednotlivých stavů průběhu synchronizace v přehledné grafické podobě

- v rámci napojení a integrace na jednotlivé IS a implementaci jejich synchronizací s IDM, musí IDM umožnit u každého IS následující režimy synchronizací (za předpokladu podpory na straně integrovaného 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* – synchronizace vždy jen konkrétní identity na vyžádání, která se provede okamžitě
    - *ověřovací synchronizace* – synchronizace vytvoří 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 v IDM systému

- IDM musí obsahovat historii běhu všech synchronizací – jednotlivé běhy synchronizací musí být zaznamenány v historii dostupné v IDM. U plné synchronizace musí historie obsahovat odkazy na objekty v IDM, které byly synchronizované včetně logu, co bylo u těchto objektů synchronizací změněno. V případě změnové synchronizace musí být navíc v historii informace o události, která synchronizaci vyvolala
- IDM musí obsahovat správu jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možno zpracovat, nastavení časového intervalu spouštění a nastavení intervalu odstávky

Požadavky na workflow

- IDM musí podporovat kompletně elektronický schvalovací proces pro udělování přístupových oprávnění uživatelům a jejich následnou evidenci. Schvalovací workflow musí být založeno na funkcích elektronických formulářů s tím, že Objednatel preferuje podepisování s využitím kvalifikovaných elektronických podpisů
- IDM musí obsahovat integrované workflow pro řízení životního cyklu změn identit a schvalování změn s min. následujícími funkcemi:
    - zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným, jak pro dotčeného uživatele, tak i pro podřízené pracovníky
    - sledování stavu vyřizování požadavků
    - možnost schválení i zamítnutí požadavků včetně možnosti uvedení odůvodnění formou komentáře u obou variant
    - odesílání schvalovateli upozornění formou emailové notifikace
    - schvalovatelé si mohou zobrazit přehled úloh čekajících na schválení o vícekrokové schvalovací workflow na základě podmínek
    - schvalovat může jednotlivec nebo více schvalovatelů (skupina schvalovatelů, která musí být definovatelná)
    - správce IDM je schopen pracovat se všemi úlohami workflow
    - řešení zastupitelnosti
    - upozornění schvalovatele při překročení termínu provedení schválení/zamítnutí
    - IDM musí být schopno zobrazit v grafické podobě workflow diagram včetně indikace stavu aktuálně běžícího workflow

Požadavky na historii, logování, audity a reporty

- IDM musí obsahovat detailní databázovou historizaci min. pro evidenci změn v identitách, referenčních objektech a jejich vzájemných vazbách

- IDM musí u historizace poskytovat data v libovolném časovém okamžiku (aktuální i zpětně v minulosti)
- IDM musí poskytovat auditní logy pro systémy typu SIEM a Log management
- IDM musí obsahovat min. následující typy logů:
    - aplikační log zaznamenávající události systému
    - auditní log zaznamenávající změny entit evidovaných v systému a změny konfigurace systému
    - synchronizační log zaznamenávající průběh synchronizací IDM s dalšími systémy
    - notifikační log zaznamenávající odeslané emailové notifikace a upozornění

- IDM musí obsahovat možnost exportu auditních reportů z údajů o identitě uložené v IDM systému včetně historických. Tyto reporty musí být min. ve formátech XML a CSV. Reporty musí obsahovat souhrnné zobrazení daných identit a jejich rolí v IS napojených na IDM, aplikačních rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti
- IDM musí všechny požadavky na změny, které provedou uživatelé provádět transakčně
- IDM musí logovat tak, aby bylo možno prokázat zpětně kdo a co v IDM změnil (v referenčních objektech, identitách, administraci a konfiguraci atd.)
- IDM musí u identit pro generování auditního reportu umožnit filtrovat dle libovolných atributů identity včetně přidružených referenčních objektů
- IDM musí umožnit generovat reporty uživatelů přiřazených aplikačním rolím
- IDM musí umožnit automatizovaně zasílat reporty e-mailem na základě konfigurovatelných pravidel
- IDM musí umožnit automatické ukládání reportů v systému IDM pro možnost pozdějšího zobrazení nebo stažení
- IDM musí umožnit porovnání změn mezi vygenerovanými reporty stejného typu
- IDM musí veškeré požadavky na změny v IDM umožnit zadávat výhradně přes webové rozhraní, tak aby bylo zajištěno úplné logování všech změn jednotlivých parametrů. Není přípustné požadavky realizovat ručními úpravami textových souborů jakou jsou např. CSV, XML atd.

Požadavky na notifikace

- IDM musí umožnit notifikovat e-mailem o vytvoření a změně identity
- IDM musí umožnit notifikovat e-mailem o vytvoření a změně referenčních objektů jako jsou systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role, vypršení hesla v Microsoft AD a vypršení platnosti certifikátu (u vypršení musí být možnost definovat s jakým časovým předstihem bude notifikace zaslána)
- IDM musí umožnit notifikovat e-mailem o problémech či konfliktech při jednotlivých synchronizacích s napojenými systémy
- IDM musí umožnit správu notifikací včetně jejich náhledu
- IDM musí umožnit v šabloně notifikací definovat příjemce, předmět a obsah upozornění. U notifikací vázaných k identitám musí IDM umožnit nastavit různé příjemce pro různé části organizační struktury

Rozhraní webových služeb

- IDM musí poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace přes webové rozhraní IDM
- IDM musí umožnit řízení uživatelských účtů a rolí v jiných systémech na principu obecné webové služby (tzn. bude možné konfigurovat konektory pro tyto webové služby pro jakýkoliv jiný integrovaný systém)
- webové služby IDM musí být definované v rozšířeném standardu WSDL a podporovat protokol SOAP
- konfigurace webových služeb musí umožnit konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet zvlášť
- IDM musí volání webových služeb logovat a logy musí být zobrazitelné přímo ve webovém rozhraní IDM
- rozhraní webových služeb musí poskytovat min. následující služby:
    - získání organizační struktury
    - získání hierarchie systematizovaných míst
    - získání seznamu identit

- získání nadřízené osoby pro daného zaměstnance
- získání seznamu aplikačních rolí
- získání seznamu uživatelů dané aplikace
- získání seznamu agend a agendových rolí přiřazených dané aplikaci
- zápis seznamu aplikačních rolí do IDM
- zápis certifikátů do IDM
- zápis a změna identit
- služba pro autorizaci pro ISZR – služba ověří validnost volání služby ISZR. Služba v IDM musí ověřovat:
  - zda je uživatel, který je v požadavku na ISZR evidován v IDM
  - zda je aplikace, která je v požadavku na ISZR evidována v IDM,
  - zda má tento uživatel v IDM nastaven přístup do aplikace, která je v požadavku na ISZR

- zda existuje v IDM v rámci evidence organizační struktury rovněž evidence pro dané OVM, které je uvedeno v požadavku na ISZR
- zda má aplikace, která je v požadavku na ISZR, v IDM povolenou agendovou činnostní roli a agendu, které jsou rovněž uvedeny v požadavku na ISZR

Obecné konektory

- IDM musí obsahovat minimálně tyto obecné konektory pro správu identit v napojených systémech a musí být možno je konfigurovat přímo z webového rozhraní IDM:
  - konektor pro spouštění CMD příkazů
  - konektor umožňující pracovat s CSV soubory
  - konektor umožňující správu identit v DB
  - konektor umožňující napojení na SOAP webové služby
  - konektor umožňující napojení na REST webové služby
  - konektor umožňující napojení na LDAPv3 (např. Microsoft AD)

- IDM musí umožnit připojení libovolného množství dalších spravovaných systémů, a to bez dalších licenčních nákladů

Napojení na Active Directory a Azure ID

- IDM musí obsahovat min. tyto funkcionality:
  - správa účtů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.)
  - podpora min. 6ti vrstvé hierarchické struktury organizačních jednotek
  - založení domovského adresáře včetně nastavení oprávnění
  - správu účtů a jejich certifikátů včetně inicializačního načtení
  - správu skupin a členství ve skupinách včetně inicializačního načtení
  - správu organizačních jednotek včetně inicializačního načtení

Napojení na IS Datacentrum 2

- IDM musí obsahovat min. tyto funkcionality:
  - vytváření a rušení identit v IS
  - spárování identit mezi IDM a IS Datacentrum 2
  - správa oprávnění pro jednotlivé uživatele agend IS
  - párování předdefinovaných funkčních míst na identity (včetně zastupujících identit)
  - párování předdefinovaných konfiguračních skupin na funkční místa (musí být možno spárovat funkční místo s více konfiguračními skupinami)

- Z tohoto personálního systému budou načítány údaje o hierarchii pracovních míst, osobách (zaměstnancích, DPP a DPČ) a tyto údaje budou pro IDM systém sloužit jako zdrojové

- Uchazeč si zajistí informace k technickému řešení a obchodní podmínky pro připojení IDM systému na IS Datacentrum 2 u dodavatele DataCentrum&consulting, a.s., kontaktní osoba: [redacted]

Další požadavky na integraci informačních systémů

- IDM musí umožnit evidenci přístupových oprávnění a rolí v integrovaných systémech a jeho částech (modulech) u jednotlivých identit (uživatelů)
- IDM musí obsahovat informace o definovaných rolích identit (dle směrnic Objednatele)
- IDM musí umožnit Objednateli definovat jednotlivé role (min. 10 rolí v každém IS)
- Evidence integrovaných systémů musí vést pro každý integrovaný systém alespoň tyto údaje:
    - název – označení integrovaného systému (povinná hodnota)
    - kód ISVS – číselný kód přidělený Informačním systémem o informačních systémech veřejné správy (nepovinná hodnota)
    - popis – slovní popis současného stavu a účelu provozování integrovaného systému
    - koncepce – informace o způsobu využívání (koncepce rozvoje nebo ukončení životního cyklu)
    - kategorie – zařazení integrovaného systému do kategorie výběrem z číselníku, kategorie mohou být uživatelsky definovatelné a upravovatelné
    - stav integrovaného systému – evidence stavu životního cyklu systému („zkušební provoz", ostrý provoz", „ukončování provozu", provoz ukončen")
    - využívané technické prostředky – evidence technických prostředků jako jsou servery, databáze, systémové prostředky výběrem z uživatelsky definovatelného číselníku
    - zálohování – popis způsobu a frekvence zálohování, výběr z číselníku

Požadavky na evidenci v nenapojených (neinteqrovaných) IS, aplikacích a systémech (dále jen NIS)

- IDM musí umožnit evidenci přístupových oprávnění a rolí v NIS a jeho částech (modulech) u jednotlivých identit (uživatelů)
- IDM musí obsahovat informace o definovaných rolích identit (dle směrnic Objednatele)
- IDM musí umožnit Objednateli definovat jednotlivé role (min. 10 rolí v každém IS)
- IDM musí obsahovat informace o přidělených oprávněních a rolích identitám v IDM Evidence NIS musí vést pro každý NIS alespoň tyto údaje:
    - název – označení NIS (povinná hodnota)
    - popis – slovní popis současného stavu a účelu provozování NIS
    - koncepce – informace o způsobu využívání (koncepce rozvoje nebo ukončení životního cyklu)
    - kategorie – zařazení NIS do kategorie výběrem z číselníku, kategorie mohou být uživatelsky definovatelné a upravovatelné
    - stav NIS – evidence stavu životního cyklu nenapojeného systému („zkušební provoz", ostrý provoz", „ukončování provozu", provoz ukončen")
    - využívané technické prostředky – evidence technických prostředků jako jsou servery, databáze, systémové prostředky výběrem z uživatelsky definovatelného číselníku
    - zálohování – popis způsobu a frekvence zálohování, výběr z číselníku

- Vazby na jiné IS a NIS – označení jiných IS, na jejichž funkčnosti závisí provoz nenapojeného IS, výběr z číselníku
- U každého evidovaného NIS musí být možno přidávat vlastní atributy a podatributy ve formě stromové struktury reprezentující různé moduly a části NIS
- U každého atributu a podatributu musí být možné evidovat, jaké oprávnění (čtení/zápis) a roli v něm uživatel (identita) má
- IDM musí umožnit provádět evidenci oprávnění v NIS nadřízeným uživatelům (vedoucí odboru dle organizační struktury) a administrátorům NIS

- IDM musí umožnit evidenci oprávnění v NIS zobrazit v přehledné formě na kartě uživatele, pro dané uživatele (identity) a veškeré nadřízené uživatele dle organizační struktury
- IDM musí umožnit výstup přehledu z evidence NIS určeného k tisku a uchování
- IDM musí umožnit filtrování a třídění v evidenci NIS podle všech dostupných polí
- IDM musí umožnit definovat vlastní sestavy k tisku z evidence NIS
- IDM musí umožnit exportovat evidenci z NIS min. do formátu CSV

Implementace IDM

Poskytovatel musí dodat plně funkční systém, kompletně zprovozněný a nakonfigurovaný dle požadavků uvedených v této zadávací dokumentaci. Způsob a postup implementace bude vycházet z projektové dokumentace zpracované uchazečem v rámci dodávky. Projektová dokumentace použitá pro implementaci IDM musí být odsouhlasena Objednatelem.

Předimplementační etapa

- zpracování implementačního projektu – Objednatel zajistí poskytnutí potřebné součinnosti ze strany jeho zaměstnanců
- implementační projekt bude mít jako výstup projektovou dokumentaci ve formátu DOCX. Obsahem projektu musí být pak zejména schéma kompletního životního cyklu identit v jednotlivých integrovaných IS v prostředí Objednatele, řešení případných změn organizační struktury Objednatele, postup integrace nového informačního systému, napojení na SIEM systém Objednatele, návrh postupu řešení časově omezených vyjímek atd.
- projektová dokumentace musí být zpracována a schválena Objednatelem před zahájením realizace vlastní instalace, konfigurace IDM systému a integrace IS Objednatele
- instalace a konfigurace IDM bude realizována na zařízeních a programovém vybavení Objednatele (aplikační a databázové servery, systém SIEM, koncové stanice a mobilní zařzení, operační a databázové systémy atd.)

Implementační etapa

- napojení všech specifikovaných IS Objednatele na IDM – viz bod „Požadavky na integraci IDM s jinými systémy“
- před napojením integrovaných systémů na IDM v produkčním prostředí musí dojít k otestování v testovacím prostředí
- implementace musí probíhat prostřednictvím pracovníka Poskytovatele přímo v místě plnění, a to v pracovní době definované dále, nebylo-li dohodnuto jinak, nebo prostřednictvím pracovníka Poskytovatele vzdálenou správou
- školení administrátorů Objednatele na začátku či v průběhu testovacího provozu v místě plnění v rozsahu specifikovaném dále tak, aby byli pověření zaměstnanci Objednatele schopni obsluhovat a spravovat dodaný IDM v potřebném rozsahu pro zajištění běžného rutinního provozu
- testovací provoz po dobu min. 60 dní
- vypracování a předání veškeré dokumentace specifikované níže
- akceptace díla po testovacím provozu

Akceptační testy a zkušební provoz

Součástí akceptačních testů a zkušebního provozu musí být minimálně:

- prokázání kompletnosti a funkčnosti dodávky IDM
- doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost
- před akceptací a předáním díla proběhne 60 denní zkušební provoz. Pokud se vyskytnou během testování nebo zkušebního provozu závady, uchazeč je povinen závady odstranit nejpozději do 2 pracovních dnů

- v průběhu zkušebního provozu může Objednatel průběžně posílat uchazeči požadavky na úpravy SW konfigurace, nejpozději však do konce 55. dne zkušebního provozu a uchazeč musí požadované změny realizovat (pokud to je technicky možné a není to v rozporu s jinou požadovanou funkcionalitou IDM)
- akceptací díla se rozumí oboustranné odsouhlasení předávacího protokolu po dokončení testovacího provozu, splnění všech doplňujících testů a odsouhlasených úpravách v konfiguraci IDM

Školení administrátorů Objednatele

Poskytovatel zajistí školení administrátorů Objednatele v rozsahu minimálně dle následujících požadavků:

- první část školení v průběhu instalace a konfigurace před zahájením zkušebního provozu pro administrátory v rozsahu max. 12 hodin rozdělených do 3 dnů v místě plnění. Školení proběhne v rozsahu potřebném pro provoz a údržbu systému (ukázka prostředí, popis a vysvětlení architektury IDM, hlavních principů a jednotlivých částí systému, vysvětlení konfigurace a její úpravy atd.)
- druhá část školení na začátku zkušebního provozu (v prvních 3 dnech) pro administrátory v celkovém rozsahu 8 hodin v místě plnění. Školení proběhne v rozsahu potřebném pro detailní obeznámení s aktuální konfigurací IDM a integračních vazeb na IS Objednatele. Současně bude předvedeno rozhraní pro uživatele (změna hesla, žádost o změnu aplikační role a úrovně oprávnění atd.)
- celkové náklady na obě části školení musí být zahrnuty v nabídkové ceně

Provozní a technická dokumentace

Poskytovatel po úspěšné instalaci, konfiguraci a zkušebním provozu IDM vypracuje a dodá Objednateli v písemné podobě podrobnou dokumentaci (ve formátu DOCX) k IDM systému.

- *provozní dokumentace* musí minimálně obsahovat popis a postupy vedoucí k nastavení systému IDM do takového stavu, aby jej bylo možno po instalaci provozovat na základní úrovni. Součástí provozní dokumentace musí být detailní popis integračních vazeb na jednotlivé IS, které byly součástí akceptace díla a popis provozních postupů pro zajištění správného, bezchybného a bezpečného provozování IDM systému. Dokument bude mít formu textového popisu doplněného o obrazová schémata a zdrojové kódy skriptů, konfiguračních souborů apod. a bude min. obsahovat:
    - konfiguraci sítě (IPv4, IPv6), nastavení připojení a komunikace na další systémy (např.DB, web server,...),
    - nastavení portů na kterých služba naslouchá, kam odesílá data...,
    - spuštění potřebných modulů, registrování knihoven, úprava registrů OS Windows atd.,
    - nastavení automatických úloh, nastavení systémových účtů atd.

- *technická dokumentace* musí obsahovat popis technické specifikace všech klíčových částí/komponent systému, jejich úkol, význam a účel (jakou platformou jsou jednotlivé komponenty zajištěny – software, agenti, typy použitých serverů, moduly, zdroje atd). Dále popis schéma systému, popis kompletní aktuální konfigurace, parametrů a nastavení jednotlivých částí systému, tak aby IDM systém bylo možno nadále provozovat a spravovat. Cílem dokumentu je popsat a zdokumentovat technickou stránku a aktuální konfiguraci IDM systému. Dokument bude mít formu textového popisu doplněného o obrazová schémata a zdrojové kódy skriptů, konfiguračních souborů apod.
- *dokumentace popisující restart a obnovu* musí min. obsahovat posloupnost všech kroků (co, kde a jak udělat), aby bylo možné provést bezpečný restart (např. informování uživatelů, ověření odhlášení uživatelů, provedení zálohy, samotný restart systému, kontrola funkčnosti). Dále posloupnost všech kroků (co, kde a jak udělat), aby bylo možné systém obnovit do jeho plně funkčního stavu po jeho selhání (např. obnova ze zálohy). Cílem dokumentu je popsat a zdokumentovat postupy a konkrétní kroky, které povedou k bezpečnému restartu nebo obnově systému. Dokument bude mít formu textového popisu doplněného o obrazová schémata a zdrojové kódy skriptů, konfiguračních souborů apod.
- *dokumentace popisující monitoring* musí obsahovat výčet logovaných událostí (např. přihlášení/odhlášení, přidělení/odebrání oprávnění, synchronizace atd.) Dále popis práce s legovanými událostmi (umístění souboru, doba uložení, vzdálený server atd.) a specifikaci logovacího protokolu (sys-

log, snmp atd.). Cílem dokumentuje popsat a zdokumentovat monitoring události. Dokument bude mít formu textového popisu doplněného o obrazová schémata a zdrojové kódy skriptů, konfiguračních souborů apod.

- Veškerá dokumentace a příručky se po předání Objednateli stává jeho majetkem a může s nimi nakládat dle svých potřeb.

Technická podpora v průběhu testovacího provozu

Poskytovatel musí v průběhu testovacího provozu (min. po dobu 60 dní) zajišťovat podporu k systému IDM v minimálním rozsahu:

- zajištění kompletní instalace pravidelných aktualizací výrobce IDM formou upgrade, update, patch včetně legislativních aktualizací (aktualizace vyvolaná vývojem operačních systémů, změnou nebo vydáním nových nařízení EU, zákonů, vyhlášek, nařízení vlády, metodických pokynů atd.) – po dohodě s Objednatelem
- zajištění funkčního stavu IDM systému (řešení závad, anomálií, vad vzniklých bez zjevného zapříčinění nebo důvodu na straně Objednatele atd.)
- poskytnutí potřebné součinnosti k zachování funkčního propojení se všemi integrovanými IS viz „Požadavky na integraci IDM s jinými systémy (a to i v případě, že dojde ke změně v připojených IS formou jejich aktualizací)
- poskytování konzultací ke správnému a efektivnímu provozování a užití IDM systému formou telefonických nebo emailových konzultací nebo vzdáleným přístupem, a to nejpozději do 3 pracovních dní od doručení žádosti Objednatele. Za doručenou žádost se považuje požadavek zaslaný na kontaktní email Poskytovatele [redacted] v pracovních dnech v době od 8:00 do 18:00 hod. (pokud není dohodnuto jinak).

ČÁST II. Privileged Access Management (PAM)

Obecné požadavky na PAM

- Zlepšení efektivity prostřednictvím automatizace správy privilegovaných účtů
- Zvýšení bezpečnosti řízením privilegovaných identit a jejich přístupů a následném auditingu a reportingu
- Zvýšení bezpečnosti v prostředí zadavatele prostřednictvím umožnění privilegovaným uživatelům žádat o udělení oprávnění na používání konkrétních privilegovaných účtů
- Zvýšení bezpečnosti prostředí zadavatele prostřednictvím kontroly síly přístupových hesel a kontroly nad jejich pravidelnou obměnou
- Existence webového rozhraní, které umožní uživatelům žádat o přístupy nebo oprávnění, schvalovat žádosti a měnit hesla
- Správa min. **30 uživatelských účtů** s privilegovanými přístupy

Systémy a uživatelské účty s požadovanou integrací do PAM

V následující tabulce je uveden seznam systémů a typů uživatelských účtů, které Objednatel požaduje napojit do PAM. V tabulce je uveden způsob napojení cílového systému a další parametry napojení do PAM.

Systém/Aplikace	Typ	Způsob napojení	Uživatelské účty	Nahrávat sezení	Dostupnost	Workflow	Skupiny s přístupem
Microsoft AD	Výchozí doménový účet	RDP	Administrator	ANO	Velice omezená	Schválení	PAM_MGMT
MS Exchange Server	Výchozí účet	Heslo	Administrator	NE	Velice omezená	Schválení	PAM_MGMT
OS Linux	Výchozí účet	SSH	root	ANO	Omezená	Komentář	PAM_INT, PAM_EXT
OS Windows	Technické doménové účty s RDP	RDP	ts-admin ts-test1	ANO	Omezená	Komentář	PAM_INT, PAM_EXT
OS Windows	Servisní účty	Heslo	cortado ictgroup prenos qradar spravce testAD totalservice veeam	NE	Velice omezená	Komentář	PAM_MGMT
Oracle DB	Systémové účty	Heslo	SYS SYSTEM	NE	Velice omezená	Schválení	PAM_MGMT
MS SQL DB	Systémové účty	Heslo	sa	NE	Velice omezená	Schválení	PAM_MGMT
VMware	Systémové účty	Heslo	root administrator	NE	Velice omezená	Schválení	PAM_MGMT
IBM QRadar	Systémové účty	SSH Heslo	root Admin	ANO	Omezená	Komentář	PAM_BEZP
IBM Guardium	Systémové účty	SSH Heslo Heslo	cli accessmgr Admin	ANO	Omezená	Komentář	PAM_BEZP
Fortigate FW	Systémové účty	Heslo	Admin	NE	Velice omezená	Schválení	PAM_MGMT
Cisco iOS	Systémové účty	SSH	cisco	ANO	Velice omezená	Schválení	PAM_MGMT

Rozdělení uživatelů do skupin v PAM řešení

PAM systém musí umožnit spravovat min. 30 účtů s vysokými přístupovými právy (administrátorské účty, správci systémů, root, speciální uživatelé atd.)

Níže je uveden obecný požadavek na uspořádání účtů jejich rozdělení do skupin v systému PAM řešení.

Skupiny použité v PAM budou reflektovány v Microsoft AD Objednatele a je požadována synchronizace těchto skupin uživatelů s Microsoft AD.

PAM systém musí podporovat alespoň jeden uživatelský účet s místním ověřováním (přihlášení není ověření pomocí LDAP protokolu), tak aby bylo možné se do systému PAM přihlásit i v případě výpadku Microsoft AD. Tento účet nebude využíván v běžné provozní praxi a bude nadstandardně zabezpečen.

#	Organizace	Osoba	Skupiny
1	-	Administrator	-
2	MČP 2	pracovník 1	PAM_MGMT
3	MČP 2	pracovník 2	PAM_MGMT
4	MČP 2	pracovník 3	PAM_INT
5	MČP 2		PAM_INT
6	MČP 2		PAM_INT
7	MČP 2	pracovník n	PAM_INT
8			
9			
10			
11	externí dodavatel 1	pracovník 1	PAM_EXT
12	externí dodavatel 1	pracovník 2	PAM_EXT
13	externí dodavetel 2	pracovník 1	PAM_EXT
14	externí dodavetel 2	pracovník 2	PAM_EXT
15	externí dodavetel 2	pracovník 3	PAM_EXT
16	externí dodavetel 2	pracovník 4	PAM_EXT
17	externí dodavetel 3	pracovník 1	PAM_BEZP
18	externí dodavatel n	pracovník 1	PAM_BEZP
19			

Workflow pro práci s PAM

- PAM systém musí podporovat tvorbu, správu a spouštění požadovaných workflow pro řízení životního cyklu účtu s privilegovanými právy.
- možnost přiřazení workflow pro konkrétní privilegované účty
- workflow musí umožnit „zapůjčení" privilegovaného účtu nebo speciálního aplikačního účtu konkrétnímu uživateli na přesně definovaný časový úsek s automatickým odebráním po uplynutí definované doby
- každé workflow je možné opatřit komentářem

Požadované typy workflow:

Schválení

Workflow zajišťuje pro vybrané uživatelské účty nutnost schválení oprávněnou osobou před jeho použitím. Schválení probíhá přímo v řešení PAM s provedením auditního záznamu, včetně komentářů a důvodů schválení/zamítnutí. Dostupnost těchto účtů je viditelné všem uživatelům, včetně označení nutného schvalovacího procesu. Jako oprávněnou osobu se pro jednotné schvalovací workflow lze definovat i skupinu uživatelů (Microsoft AD).

V případě potřeby lze jednotné schvalovací workflow rozdělit a vytvořit jeho samostatné instance s omezením na konkrétní oprávněné osoby.

Je požadována podpora i víceúrovňových schvalovacích workflow.

Workflow „Schválení" musí implementovat povinnost „zapůjčení" uživatelského účtu na určitý, definovaný časový úsek, který si uživatel stanovuje při vkládání komentáře. Během tohoto časového úseku je uživatelský účet „zapůjčen" k užívání vždy pouze jednomu uživateli.

Komentář

Workflow vynucuje při „zapůjčení" účtu zadání komentáře se zdůvodněním k zápůjčce uživatelského účtu. Komentář je zadán přímo v řešení PAM a je uložen v auditním logu.

Workflow „Komentář" také obsahuje povinnost „zapůjčení" uživatelského účtu na určitý časový úsek, který si uživatel stanovuje při vkládání komentáře. V tento úsek je uživatelský účet propůjčen k užívání vždy pouze jednomu uživateli.

Další požadované funkcionality a vlastnosti systému PAM

- podpora automatické změny hesel pro vybrané účty s možností definovat frekvenci těchto změn
- systémová podpora procesu zálohování interní databáze PAM při změnách interních dat
- systémová podpora těchto způsobů napojení na cílové aplikační systémy, jejichž privilegované účty budou řízeny PAM:

- Remote Desktop Protocol (RDP)
  Servery s operačním systémem Microsoft Windows je možné napojit pomocí RDP protokolu, kdy PAM řešení musí umožňovat přímé spuštění výchozího RDP klienta a automaticky do něj předá uživatelské jméno a heslo, tak aby uživatel systému PAM jej nemohl získat.

- (Secure Shell) SSH
  Servery s operačním systémem Linux/Unix a appliance např. síťových prvků je možné napojit pomocí SSH protokolu, kdy PAM řešení musí umožňovat přímé spuštění

výchozího SSH klienta a automaticky do něj předá uživatelské jméno a heslo, tak aby uživatel systému PAM jej nemohl získat.

- Telnet

  Servery s operačním systémem Linux/Unix a appliance např. síťových prvků je možné napojit pomocí SSH protokolu, kdy PAM řešení musí umožňovat přímé spuštění výchozího SSH klienta a automaticky do něj předá uživatelské jméno a heslo, tak aby uživatel systému PAM jej nemohl získat.

- Heslo

  Pro uživatelské účty, kdy není možné nebo není záhodno využívat ostatní typy napojení doporučujeme využít tento typ. Při nutnosti přístupu k uživatelskému jménu a heslu tohoto uživatelského účtu je heslo zobrazeno v rozhraní PAM. Vzhledem k možnému zneužití díky zobrazení hesla, doporučujeme tento typ zajistit dodatečnou ochranou, jako je například nutnost schválení.

Požadavky na implementaci a zálohování systému PAM

- Požadujeme, aby finálně vybrané řešení podporovalo a bylo implementováno distribuovanou architekturou, tedy minimálně oddělení aplikační části a databáze nebo uložiště spravovaných uživatelských účtů.
- Požadujeme formu implementace pomocí virtuální appliance nebo virtuálního serveru do vlastní infrastruktury zadavatele, provozované na platformě VMware. Virtuální nasazení je preferováno taktéž z důvodu jednoduchého zálohování samotné appliance nebo serveru pomocí tzv. snapshotů.
- Požadujeme využít zadavatelem využívaných databázových technologií (Oracle, MSSQL) v rámci implementace PAM řešení, pokud řešení využívá k ukládání spravovaných uživatelských účtů tyto typy databázových technologií. Toto doporučení plyne z využití již existujících DB clusterů s vyřešeným procesem zálohování a obnovy.
- Požadujeme využití externího uložiště pro ukládání nahrávek sezení a automatických záloh řešení PAM.
- Požadujeme podporu zálohování systémových dat PAM na proces automatické změny hesel s možností nastavení i dalších záloh v určeném intervalu.
- Požadujeme podporu zálohování na třech úrovních: aplikace, databáze (uložiště), uložiště nahrávek sezení.
- Požadujeme podporu šifrování záloh pro jejich zabezpečení.

Část III. Harmonogram, plán implementace IDM+PAM a odstávek

Objednatel vyžaduje dodržení následujícího harmonogramu plnění, jenž začíná v čase T a v němž jsou uvedeny maximální možné lhůty pro jednotlivé významné milníky.

Poskytovatel připraví podrobný harmonogram prací před započetím realizace plnění veřejné zakázky v čase T, který musí schválit Objednatel.

ID	Popis	Čas	Celková doba (dny)	Fakturační milník v návaznosti na čl. 5.1 smlouvy
1	Zahájení – část IDM + PAM	T	T+5	Ne
2	Dodávka licencí, technické podpory výrobce na 24 měsíců a instalace systémů IDM a PAM v prostředí Objednatele	T	T+30	Ano, 50%
3	Implementační projekt za poskytnutí součinnosti zaměstnanců Objednatele z dotčených odborů a zhotovení projektové dokumentace k IDM a PAM	T	T+30	Ne
4	Implementace integrace IDM na MS AD a personální system Datacentrum 2 + školení administrátorů	T	T+60	Ano, 35%
5	Zkušební provoz 2 měsíce, asistence a podpora, vypracování a předání dokumentace	T	T+120	Ne
6	Zapracování připomínek a předání finální verze projektové dokumentace Objednateli, akceptace Objednatelem	T	T+125	Ano, 15%

Bez odstávkové práce mohou probíhat za běžného provozu. Práce, jež omezují provoz informačních systémů Objednatele nebo vyžadují jejich odstávku, musí být prováděny mimo pracovní dobu Objednatele, nebylo-li dohodnuto jinak.

Pracovní doba, po kterou je možno pracovat v místě plnění:

- pondělí a středa 8:00 – 17:30
- úterý a čtvrtek 8:00 – 16:00
- pátek 8:00 – 14:00

Odstávky a práce omezující provoz je možno provádět v těchto časech po předchozí dohodě se zástupcem Objednatele:

- pondělí a středa 17:30 - 20:00
- úterý a čtvrtek 15:30 - 20:00
- pátek 13:30 - 20:00

Odstávky po 20:00 hod., o víkendu nebo státním svátku je možno realizovat dle individuální domluvy se zástupce Objednatele.

Příloha Smlouvy

Příloha č. 2 - Ujednaní o ochraně a zpracování osobních údajů

Ujednání o ochraně a zpracování osobních údajů

S ohledem na předmět této Smlouvy (Smlouva o poskytování služeb bezpečnostního dohledu nad informačními systémy MČ Praha 2) smluvní strany předpokládají, že Poskytovatel bude v rámci plnění této Smlouvy zpracovávat osobní údaje, zejména o osobní údaje, zaměstnanců, občanů a/nebo smluvních partnerů správce. Toto ujednání obsahuje rovněž ujednání o zpracování osobních údajů dle čl. 28 podle NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, v platném znění (dále jen „Nařízení GDPR")

Nařízení GDPR, mezi objednatelem jako správcem osobních údajů a poskytovatelem ve smyslu smlouvy jako zpracovatelem osobních údajů, uvedená níže.

1. OBECNÉ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1.1 Objednatel jako správce osobních údajů pověřuje poskytovatele jako zpracovatele osobních údajů zpracováváním osobních údajů v rozsahu nezbytném pro plnění Smlouvy a výhradně za účelem vyplývajícím z účelu smlouvy.

1.2 Povinnosti poskytovatele týkající se ochrany osobních údajů se poskytovatel zavazuje plnit i po zániku účinnosti Smlouvy.

1.3 Poskytovatel je povinen postupovat při zpracování osobních údajů v souladu s touto smlouvou a Nařízením GDPR, a zpracovávat osobní údaje výlučně pro účel a v rozsahu, ve kterém mu byly předány a při zpracování postupovat jako odborník s řádnou péčí tak, aby neporušil žádné ustanovení Nařízením GDPR, či jiného právního předpisu nebo nezpůsobil skutečnost, která by znamenala porušení Nařízení GDPR, či jiného právního předpisu objednatelem.

1.4 V případě ukončení této smlouvy je Poskytovatel povinen předat objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li poskytovatel od objednatele písemně jiné pokyny.

1.5 Poskytovatel je povinen dbát, aby žádná osoba neutrpěla újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu osobních údajů osob před neoprávněným zasahováním do soukromého a osobního života.

1.6 Poskytovatel se zavazuje dodržovat všechny povinnosti, které mu jako zpracovateli osobních údajů vyplývají z nařízení GDPR, jakož i z interních předpisů objednatele a rozhodnutí či doporučení nebo stanovisek vydaných pro Objednatele příslušným orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu.

1.7 Za účelem plnění povinností v souvislosti s ochranou a zpracováním osobních údajů dle smlouvy se objednatel zavazuje bezodkladně po jejich obdržení poskytovat poskytovateli jakákoliv rozhodnutí či doporučení nebo stanoviska vydaná příslušným orgánem státní správy.

1.8 Poskytovatel je povinen zajistit, že zpracovávání osobních údajů probíhá v souladu s Nařízením GDPR i v tom smyslu, že v případě, že je podle Nařízení GDPR či jiného příslušného právního předpisu vyžadováno jakékoli oznámení nebo jiný úkon vůči Úřadu pro ochranu osobních údajů či jinému správnímu orgánu, upozorní na tuto skutečnost objednatele v dostatečném předstihu a v případě, že tím objednatel poskytovatele pověří a zmocní, zajistí provedení těchto úkonů.

1.9 Pokud poskytovatel zjistí, že objednatel porušuje povinnosti stanovené Nařízením GDPR, je povinen jej na to neprodleně upozornit.

1.10 V případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování osobních údajů poskytovatelem či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu k zpracování osobních údajů poskytovatelem, je poskytovatel tuto skutečnost povinen okamžitě oznámit objednateli a poskytnout mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového procesu, včetně kopií veškeré dokumentace (kontrolní protokol, zpráva o přijatých opatřeních k nápravě, atp.).

1.11 Poskytovatel není oprávněn osobní údaje jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle této Smlouvy.

1.12 Poskytovatel je dále povinen řádně vypořádávat požadavky a nároky vznesené subjekty údajů.

1.13 Poskytovatel je povinen umožnit objednateli na vyžádání kontrolu dodržování povinností dle této přílohy smlouvy, zejména přístupy do prostor, v nichž jsou osobní údaje uchovávány, předložení seznamu osob s přístupem k osobním údajům či doložení, že veškeré osoby přistupující k osobním údajům splňují požadavky pověřené osoby. Poskytovatel je rovněž povinen umožnit objednateli přístup do databáze s osobními údaji předáním přístupových údajů, a to vždy jednorázově na základě konkrétní žádosti objednatele.

2. ROZSAH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

2.1 Poskytovatel bude zpracovávat osobní údaje pouze v rozsahu nezbytném pro plnění této Smlouvy a pro výkon práv a povinností poskytovatele dle smlouvy.

2.2 Zpracování osobních údajů je poskytovatel povinen provádět pouze v následujícím rozsahu nezbytně nutném pro plnění práv a povinností poskytovatele dle Smlouvy:

2.2.1 identifikační údaje (zejména jméno a příjmení, datum narození a akademický titul);

2.2.2 kontaktní údaje (zejména e-mailová adresa, telefonní číslo);

2.2.3 údaje související s pracovním poměrem (zejména údaje o plnění pracovních povinností a pracovním zařazení);

2.2.4 údaje o využívání služeb.

3. ZÁRUKY O TECHNICKÉM A ORGANIZAČNÍM ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ EVIDOVANÝCH OSOB

3.1 Poskytovatel je povinen zabezpečit v rozsahu služeb poskytovaných dle této smlouvy řádnou technickou a organizační ochranu zpracovávaných osobních údajů způsobem stanoveným v Nařízení GDPR či v jiných právních předpisech.

3.2 Poskytovatel je povinen při zpracování osobních údajů zajistit ochranu osobních údajů minimálně na takové úrovni, aby byly dodrženy veškeré záruky o technickém a organizačním zabezpečení osobních údajů uvedené níže v této příloze smlouvy.

3.3 Poskytovatel se zavazuje přijmout taková opatření, aby nemohlo dojít k neoprávněnému ani nahodilému přístupu k osobním údajům, k jejich úplné ani částečné změně, zničení či ztrátě, neoprávněným přenosům či sdružení s jinými osobními údaji, či k jinému neoprávněnému zpracování v rozporu se Smlouvou. Poskytovatel zároveň užije taková opatření, která umožní určit a ověřit, komu byly osobní údaje předány. Tato povinnost platí i po ukončení zpracování osobních údajů.

3.4 Poskytovatel se za účelem ochrany osobních údajů zavazuje zajistit zejména, že:

3.4.1 Přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru k Poskytovateli, budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním osobních údajů a jejich zpracováním a dále budou prokazatelně poučeny o dalších povinnostech, které jsou povinny dodržovat tak, aby nedošlo k porušení Nařízení GDPR či jiných právních předpisů (dále jen „**pověřené osoby**"). Splnění těchto povinností zajistí Poskytovatel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání. Poskytovatel nesvěří zpracování osobních údajů jakékoliv třetí osobě bez předchozího písemného souhlasu poskytovatele a vždy vhodným způsobem zajistí, že jeho zaměstnanci a jiné osoby, které budou zpracovávat osobní údaje na základě smlouvy s poskytovatelem, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu poskytovatelem stanoveném a odpovídajícím této příloze smlouvy a za podmínek Nařízení GDPR, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob.

3.4.2 Při zpracování osobních údajů budou osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat a s využitím programového vybavení tak, aby byl vyloučen neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob než pověřených zaměstnanců Poskytovatele, jedná-li se o osobní údaje v elektronické podobě.

3.4.3 Při zpracování osobních údajů v jiné, než elektronické podobě budou osobní údaje uchovány v objednatelem poskytnutých objektech a místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby, a bude vedena řádná evidence o pohybu dokumentů obsahujících osobní údaje.

3.4.4 Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto smlouvou. Přístup bude umožněn na základě přístupových kódů či hesel, tak aby byl každý přístup zaznamenán; osobní údaje budou pravidelně zálohovány.

3.5 Poskytovatel se zavazuje na písemnou a odůvodněnou žádost objednatele přijmout v přiměřené lhůtě další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.

3.6 Poskytovatel se zavazuje zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s Nařízením GDPR a jinými právními předpisy, přičemž zajišťuje, kontroluje a odpovídá zejména za:

3.6.1 plnění pokynů pro zpracování osobních údajů specialisty poskytovatele, které mají bezprostřední přístup k osobním údajům,

3.6.2 zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,

3.6.3 zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a

3.6.4 opatření, která umožní určit a ověřit, komu byly osobní údaje zpřístupněny nebo předány.

3.7 V případě zjištění porušení záruk dle této přílohy smlouvy je poskytovatel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do tří (3) pracovních dnů poté, co je k tomu objednatelem vyzván.

3.8 V oblasti automatizovaného zpracování osobních údajů je poskytovatel v rámci opatření podle předchozích odstavců povinen také:

3.8.1 zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby,

3.8.2 zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,

3.8.3 pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a zabránit neoprávněnému přístupu k datovým nosičům.

4. DOBA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A ODPOVĚDNOST POSKYTOVATELE

4.1 Poskytovatel bude osobní údaje zpracovávat po dobu účinnosti Smlouvy.

4.2 Po uplynutí doby zpracování osobních údajů podle odstavce 4.1 této přílohy smlouvy mohou být osobní údaje poskytovatelem zpracovávány pouze v nezbytném rozsahu a výhradně za účelem ochrany práv a právem chráněných zájmů objednatele a poskytovatele, nebo jiné dotčené osoby. Poskytovatel jednotlivé osobní údaje zlikviduje, jakmile pomine účel, pro který byly osobni údaje zpracovávány.

4.3 Poskytovatel odpovídá subjektům údajů za škodu a nemajetkovou újmu způsobenou porušením povinnosti poskytovatele v souvislosti se zpracováním osobních údajů. Poskytovatel dále odpovídá objednateli za škodu a nemajetkovou újmu způsobenou vznikem povinnosti objednatele hradit v souvislosti se zpracováním osobních údajů na základě smlouvy nebo v souvislosti s ní jakoukoli náhradu škody a nemajetkové újmy subjektu osobních údajů nebo pokutu Úřadu pro ochranu osobních údajů či jinému správnímu orgánu v důsledku porušení povinností uložených poskytovateli zákonem nebo smlouvou.

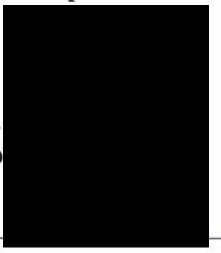
4.4 Poskytovatel se zavazuje trvale vyhodnocovat plnění zákonných povinností souvisejících se zpracováním osobních údajů při provozu infrastruktury a průběžně navrhovat veškerá nezbytná opatření a změny ujednání o zpracování osobních údajů, které zajistí řádné plnění veškerých povinností poskytovatele souvisejících s ochranou osobních údajů.

Doložka
potvrzující, že byly splněny podmínky platnosti právního úkonu, ve smyslu ust. § 43 zákona č. 131/2000 Sb., o hlavním městě Praze, ve znění pozdějších předpisů

Zveřejněno: od 22.7.2021 do 5.8.2021

~~Schváleno~~ / odsouhlaseno usnesením ~~ZMČ~~ RMČ č. 586 ze dne 23.8.2021

vedoucí odboru: Ing. Petr Štěpán



.....
podp

Nehodící se škrtněte