Příloha č. 3 Implementace systému pro autentifikaci a autorizaci uživatelů (IAM) - Technická specifikace

Vymezení předmětu plnění veřejné zakázky

1. Předmět plnění veřejné zakázky

(1) Předmětem veřejné zakázky je dodávka a implementace systému pro autentizaci a autorizaci uživatelů (IAM) tj. implementace technologických nástrojů podporujících řízení přístupů a oprávnění uživatelů úřadu k vnitřním zdrojům informačních systémů úřadu a jednotnému identitnímu prostoru veřejné správy. Součástí plnění je i dodávka a implementace integrační platformy ESB (Enterprise Service Bus), která bude tvořit základ „servisní architektury“ IS úřadu a která bude vybraným agendám (jejich IS) poskytovat služby integrační sběrnice včetně možnosti napojení na informační systém základních registrů (ISZR). V rámci realizace předmětu plnění tedy dojde k:

(a) Implementaci systému pro autentizaci a autorizaci uživatelů – „Identity a Access management“ (IAM)

(b) Vytvoření nástroje pro plánování a řízení organizační struktury úřadu

(c) Připojení nástroje pro správu identit ke stávajícímu personálnímu systému FLUX, jako autoritativnímu zdroji dat o uživatelích

(d) Připojení zdrojů dat o uživatelích identifikovaných v rámci analýzy

(e) Připojení systému IAM k ovládaným lokálním agendovým systémům

(f) Vytvoření integrační platformy ESB

(g) Integrace s ISZR

2. Popis stávajícího stavu

(1) Informační infrastruktura Magistrátu města Karlovy Vary je provozována v technologickém centru (dále také jen „TC“) v provozním režimu 5×12.

(2) Technologické centrum zahrnuje následující vrstvy:

(a) komunikační infrastruktura – zajišťuje komunikaci vrstev TC uvnitř i vně;

(b) systémová infrastruktura – zajišťuje výpočetní výkon a prostor pro ukládání dat aplikací a služeb;

(c) systémové služby – zajišťují spolupráci mezi jednotlivými systémy, zajišťují bezpečný přístup ke službám a aplikacím, apod.;

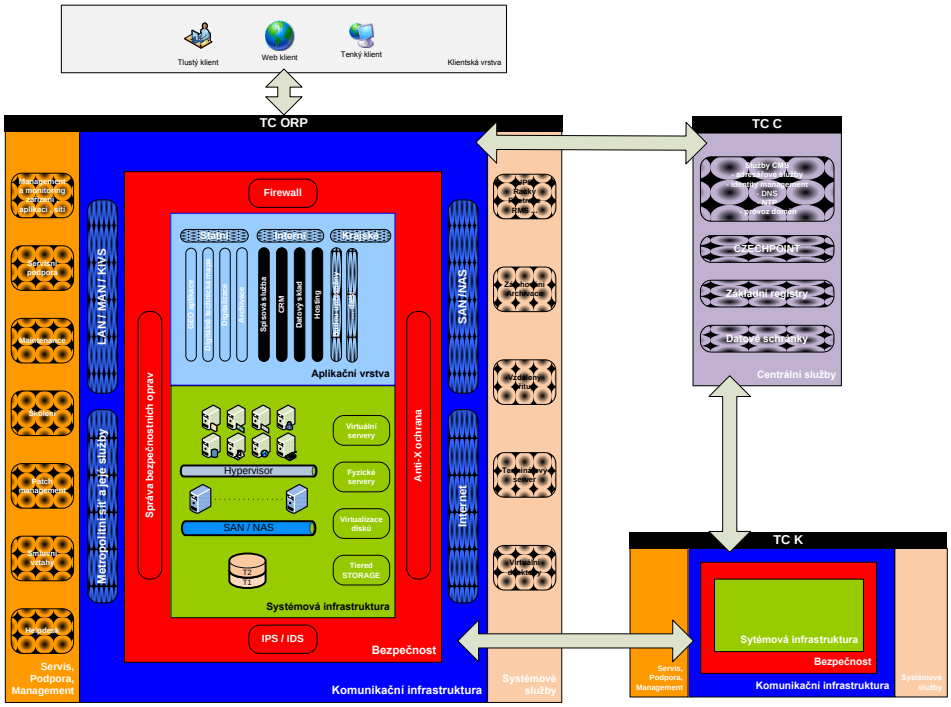
(d) aplikační vrstva – obsahuje aplikační logiky hostujících aplikací, včetně databázových serverů;

(e) bezpečnost – zajišťuje minimalizaci možných bezpečnostních incidentů;

(f) servis, podpora a řízení infrastruktury TC;

(g) klientská – zohledňuje a reprezentuje klientovi služby a jeho uživatelské rozhraní.

(3) Schématický diagram technologického centra a návaznosti na ostatní systémy je uveden níže:



(4) Zálohování a obnova dat jsou v konceptu TC řešeny na několika úrovních. Vrstva diskové virtualizace nabízí vlastnosti vytváření a práce se zálohami jako jsou:

(a) Práce s časovými snímky dat;

(b) Konzistentní snapshoty – pomocí agentů nainstalovaných na jednotlivých klientských serverech lze takto provádět také konzistentní snapshoty pro tyto systémy: IBM DB2 UDB, Informix, Microsoft SQL Server, Oracle, Pervasive.SQL, Sybase, SAP, IBM Lotus Notes/Domino, Microsoft Exchange, Microsoft VSS, Novell GroupWise a souborové systémy (AIX, HP UX, Linux, NetWare, Solaris a Windows);

(c) Možnost zálohování přímo z vytvořených snapshotů pomocí zálohovacího software.

(5) Snapshoty (plnohodnotné kopie zálohovaných dat jednoduše zpřístupnitelné pro plné použití nebo obnovu částí dat) budou vytvářeny nad LUNy jak na primárním, tak na sekundárním diskovém úložišti. Mohou být tedy vytvářeny podle potřeby i na LUNech, do kterých budou ukládána dat z aplikačních serverů obcí a organizací.

(6) V současné době využívá Město Karlovy Vary jednu technologickou místnost vybavenou zabezpečovacím systémem včetně zhášecího sytému, klimatizací, záložním zdrojem, diesel agregátem, blade servery připojenými k FC SAN úložištím EVA 4100, MSA 2000, samostatnými servery s lokálními úložišti s operačními systémy Windows 2003/2008 (Active Directory, elektronická pošta Exchange, databáze MS SQL 2005, Sharepoint 2007, ekonomickým systémem, spisovou službou, agendami úřadu a zálohovacím systémem Symantec Backup Exec). Připojení do Internetu je zabezpečeno firewallem TMG a Cisco ASA, antivirovou ochranu řeší produkt Symantec a ESET NOD32. Na blade serverech je nasazen systém virtualizace na technologii VMware verze 4. Konektivita do Internetu je v současné době 20Mb/s.

3. Popis cílového stavu a specifikace předmětu plnění

(1) Předmět plnění tvoří tři části – systém pro autentizaci a autorizaci uživatelů (IAM), integrační middleware pro napojení na ISZR a integrační platforma ESB – toto řešení jako celek pak bude tvořit základní „servisní architekturu“ úřadu.

(2) Systém pro autentizaci a autorizaci uživatelů (IAM) musí umožňovat správu uživatelů informačního systému včetně autentizace (ověření identity) a autorizace (ověření oprávnění) těchto uživatelů při přístupu k informačnímu systému úřadu i k ISZR.

(3) IAM musí být kompatibilní nebo umožňovat propojení systému s Active Directory. IAM udržuje informaci o organizačním uspořádání úřadu doplněnou o technické či externí organizace a uživatele. Organizační uspořádání je udržováno na základě informací ze stávajícího personálního systému FLUX. Technické a externí organizační jednotky a uživatelé mohou být spravováni manuálně. Takto vznikající ucelená informace o uživatelích pak musí být synchronizována do Active Directory, čímž je zajištěna centrální správa celého IAM. Proti tomuto IAM je pak realizována autentizace a autorizace uživatelů přistupujících k jednotlivým komponentám informačního systému úřadu. Pro autentizaci je využíván Active Directory, pro autorizaci IAM.

(4) IAM musí umožnit udržovat informaci o agendách, činnostech a rolích, ve kterých má úřad působnost. Tato informace musí být synchronizována prostřednictvím integračního middleware z ISZR (z RPP). K takto získané informaci bude v IAM doplněna konkrétní skladba oprávnění v jednotlivých aplikacích využívaných pro pokrytí konkrétních rolí. Přiřazením konkrétní role konkrétnímu pracovníkovi bude tak najednou přiděleno jak oprávnění k základním registrům, tak oprávnění k aplikacím informačního systému úřadu.

(5) IAM musí zajišťovat řízení oprávnění v agendách MS Sharepoint.

(6) Agenda SVI, která je v současné době provozována na MMKV, je vzhledem ke svému zaměření velmi specifická a specifické je i přidělování oprávnění, které často vyžaduje znalost dat, ke kterým se oprávnění přiděluje. Z těchto důvodů nemusí být oprávnění pro SVI (vyjma přístupů k registrům) přidělována v IAM. Z IAM bude do SVI pouze předávána informace o „zániku“ (zánik pracovního poměru, rodičovská dovolená, apod.) uživatele, která bude v SVI zohledněna. Aby byl zajištěn v IAM centrální přehled o přidělených oprávněních, bude SVI předávat do IAM informace o uživatelích s přidělenými oprávněními do SVI.

(7) IAM musí umožňovat evidenci organizační struktury organizace, včetně jednotlivých pracovníků zařazených v této organizační struktuře do organizačních rolí. Zároveň musí umožnit administrátorům organizace řídit přístupová práva do evidovaných aplikací. Organizační strukturu i pracovníky musí být možné synchronizovat periodicky z personálního systému a následně přenášet a aktualizovat do systému Active Directory.

(8) IAM musí umožňovat alespoň následující funkce:

(a) evidence seznamu pracovníků a jejich zařazení do organizačních rolí (i vícenásobné - komise, krizové štáby, zastupitelé, apod.), evidování jejich kontaktů

(b) modelování stromu organizačních rolí (definování nadřízenosti a podřízenosti napříč organizační strukturou); organizační role svým významem odpovídá funkčnímu místu

(c) modelování oprávnění na úrovni organizační role nebo skupinové organizační role - přiřazení oprávnění na úrovni organizace, ne na úrovni pracovníka; pracovník přebírá oprávnění z organizační nebo skupinové role po zařazení pracovníka do této role; oprávnění pracovníka jsou dána sjednocením oprávnění ze všech organizačních rolí, ve kterých je zařazen

(d) evidence všech aplikací řízených pomocí systémů IAM

(e) administrátorské nastavení přístupových práv jednotlivým uživatelům pro jednotlivé aplikace

(f) řízení přístupových práv jednotlivých aplikací systému

(g) možnost průběžného přidávání dalších aplikací, a modelování jejich struktury oprávnění pomocí pojmenovaných atributů oprávnění a jejich hodnot

(h) sdružení skupin přístupových práv do profilů

(i) synchronizace organizační struktury a seznamu pracovníků z personálního systému Flux prostřednictvím rozhraní

(j) synchronizace organizační struktury a seznamu pracovníků do systému Active Directory, včetně zařazování do NT skupin

(k) možnost synchronizace s více AD (řízení více organizací)

(l) komunikace externích systémů (aplikací třetích stran) se systémem IAM prostřednictvím rozmanité nabídky webových služeb standardu SOAP

(m) sledování historie přidělení oprávnění

(n) časový řez aplikace - možnost přepnutí celého systém IAM zpět do určitého času - zobrazení stavu celého IAM v daném čase

(o) různé způsoby autentizace uživatelů (oproti doméně nebo vlastní IAM)

(p) pomocný nástroj pro spouštění aplikací jednotlivými uživateli, který zobrazuje jen aplikace, ke kterým má uživatel přidělené oprávnění; nástroj bude dostupný z klientské stanice uživatele (zástupce na ploše, ikona v oznamovací oblasti apod.)

(q) evidence agend, činností a rolí a nastavení přístupových práv jejich prostřednictvím

(r) možnost evidence vlastních agend i mimo číselník ISZR (např. pro popis vnitřních procesů úřadu) a jejich využití pro přidělení oprávnění

(s) zakládání emailových účtů v Exchange 2000 a vyšší

(t) možnost exportu vybraných dat - seznamy oprávnění, podklady pro telefonní seznam

(u) možnost řízení oprávnění aplikací různými způsoby – on-line čtení oprávnění z IAM, dávková synchronizace z IAM, prostřednictvím přidělování NT skupin v IAM apod.

(9) Agendy, činnosti i role v rámci IAM musí být možné svázat s organizačními rolemi a skupinovými rolemi. Lze naplnit katalog (rejstřík) agend obsahující ucelený seznam agend, činností, agendových rolí a jejich popis. Jednotlivé agendy jsou definovány ve stromové struktuře pro zajištění logického seskupení a jednodušší orientace. Ke každé agendové roli je možné přiřadit určitá oprávnění přímo nebo prostřednictvím nadřazené činnosti či agendy. Jestliže pak v IAM administrátor prováže agendové role na organizační role, automaticky tyto organizační role přebírají práva z přiřazených agendových rolí, obdobně jako je tomu například při zařazení do organizační struktury.

(10) Systém IAM musí poskytovat webové služby. Tyto webové služby umožní všem okolním systémům získávat nezbytné informace pro jejich činnost. Kromě běžných funkcí, které je možné volat přes webové služby a které poskytují např. informace o organizační struktuře, organizačních rolích, právech přiřazených pro uživatele pro jednotlivé aplikace, apod. Musí být rovněž k dispozici možnost tvorby (vývoj) služby dle požadavků např. plynoucí z předimplementační analýzy.

(11) Systém IAM musí být integrován se stávajícím personálním systémem FLUX. Integrace musí být realizována jako jednosměrná, tj. data jsou synchronizována vždy ve směru z personálního systému do IAM. Personální systém vždy vyexportuje svůj aktuální stav, který je v IAM porovnán se stavem IAM, na základě tohoto vnitřního porovnání jsou následně promítnuty změny - založení pracovníka, organizační jednotky, zařazení či vyřazení pracovníka z organizační role, apod. Tuto synchronizaci je možné spouštět: zásahem administrátora, nastavením času na pevně stanovenou dobu nebo personálním systémem pomocí webové služby. Celou synchronizaci s personálním systémem musí být možné provést zkušebně, tj. že se porovná stav obou systémů proti sobě v daném okamžiku, zjistí se všechny prováděné změny, ale vlastní aktualizace dat se neprovede do pokynu administrátora. Systém musí umožňovat předem nastavit limity, při jejichž překročení se zabrání IAM v provedení aktualizace dat a dojde k automatickému upozornění administrátora systému.

(12) Systém IAM musí být integrován s Active Directory (AD). IAM pomáhá administrátorům sítě při vytváření nových účtů, jejich aktualizaci, přiřazování do NT skupin, zakládání e-mailových účtů, apod. Vazba na AD dále spočívá v ověřování (autentizaci) jednotlivých přihlášených uživatelů při spouštění každé aplikace. IAM musí umožňovat prvotní synchronizaci všech účtů z AD, trvalou synchronizaci ve směru z IAM do AD.

(13) Přenos údajů ze systému IAM do AD musí být možné parametrizovat, tzn. že lze definovat (nastavení, skriptem, atp.), jaké položky a jak se budou přenášet. Tak je možné dosáhnout využití standardních nebo specifických polí v AD k synchronizaci a definovat jak se budou plnit (např. do pole zobrazované jméno v AD naplnit sloučení polí příjmení a jméno, popř. i bez diakritiky).

(14) IAM musí umožňovat zařazování do NT skupin a jejich vyřazování, musí být podporovány alespoň dva principy zařazování a vyřazování do/z NT skupin - přiřazení NT skupiny k aplikaci či profilu a přiřazení NT skupiny k organizační jednotce. Jestliže je k aplikaci či k profilu přiřazena NT skupina, v okamžiku, kdy je tato aplikace přiřazena uživateli, je tento uživatel automaticky přiřazen do nastavené NT skupiny. Rovněž je možné přiřazovat NT skupiny na organizační jednotky. V takovém případě pak všichni uživatelé, kteří jsou do této organizační jednotky zařazeni, i všichni zařazení do podřízených organizačních jednotek a rolí, jsou zařazeni do zadané NT skupiny. Vlastní přiřazení skupin uživatelům v AD probíhá v rámci synchronizace dat z IAM do AD.

(15) IAM musí poskytovat klientskou aplikaci s využitím standardní NTLM autentizace pro ověření uživatele. Přihlášený a ověřený uživatel má nastavena administrátorem práva pro svoji činnost v klientské aplikaci IAM. Může tak mít omezen např. přístup pouze na pořizování uživatelů za určitou organizační jednotku. Rovněž mohou být omezeny entity, ke kterým má uživatel přístup - uživatel může mít oprávnění pouze např. pro pořizování kontaktů.

(16) IAM musí umožňovat aby při spouštění aplikace, která má řízené oprávnění systémem IAM, byl uživatel autorizován nejdříve v IAM. Na základě této autorizace jsou zpravidla prostřednictvím webových služeb poskytnuta patřičná oprávnění, která již dříve administrátor uživateli přiřadil. Na základě těchto oprávnění pak spouštěná aplikace zobrazí či nezobrazí patřičnou funkcionalitu.

(17) IAM musí být integrován se stávajícím systémem Microsoft Exchange. Je vyžadována schopnost komunikace s rozšířeným schématem AD v okamžiku, kdy je nasazen MS Exchange, dále zakládat nové e-mailové účty, přičemž administrátor může stanovit logiku vytváření e-mailové adresy, která je generována při vytvoření nebo modifikaci osob v IAM. Systém IAM musí umožňovat generování skriptů pro PowerShell, jejichž spouštění a vyhodnocování chybových stavů musí provádět administrátor.

(18) IAM musí umožňovat spouštění aplikací prostřednictvím nástroje/aplikace dostupné z pracovní stanice uživatele, a zajistit jejím prostřednictvím centrální nastavení jednoduchého přístupu všech uživatelů k aplikacím. Jednotlivé aplikace mohou být spouštěny z pracovní

plochy uživatele (zástupce na ploše, ikona v oznamovací oblasti MS Windows apod.), kde jsou nabídnuty všechny pro daného uživatele přístupné aplikace. Jednotlivé aplikace i práva v těchto aplikacích nastaví příslušný administrátor aplikace. Uživatel tedy nemusí znát umístění dané aplikace a přesto ji může přes uvedený nástroj IAM spustit. Při přesunu aplikace na jiné místo změní administrátor pouze cestu v IAM.

(19) IAM musí poskytovat otevřené rozhraní tj. disponovat obecným komunikačním rozhraním, které umožňuje připojení aplikací k aplikačnímu serveru IAM pomocí technologií WebServices/SOAP. Toto komunikační rozhraní musí umožňovat plný přístup k vybraným objektům a funkcím včetně importu či exportu dat. Preferovaným způsobem komunikace je vždy využití aplikačního rozhraní - webových služeb. Pro importy dat z personálních systémů musí být k dispozici alespoň rozhraní ve formátu XML souborů, tyto soubory musí být možné ve správné struktuře importovat do IAM, čímž je provedena plná aktualizace organizační struktury, osob a jejich zařazení do organizačních rolí.

(20) IAM musí umožnit navázání jakékoli aplikace na IAM několika různými způsoby na různých úrovních. Ve všech případech musí být aplikace využívající pro přidělování oprávnění IAM založena jako aplikace v IAM, kde jsou pro ni založeny atributy oprávnění a jejich hodnoty. Atributy oprávnění reprezentují jednotlivá oprávnění a hodnoty atributů hodnoty těchto oprávnění samostatně pro každou aplikaci.

(21) IAM musí umožňovat integraci s aplikacemi třetích stran alespoň následujícími způsoby:

(a) využitím webových služeb - aplikace využívá pro čtení organizační struktury a přístupových oprávnění webových služeb, jejich prostřednictvím pak on-line čte organizační strukturu a oprávnění nebo využívá tyto služby pro synchronizaci organizační struktury a oprávnění do vlastního úložiště. Webové služby musí být popsány v detailní dokumentaci, popisující jednotlivé parametry funkcí.

(b) aktivním poskytováním oprávnění z IAM (provisioning) tzn. aktivním poskytováním dat z IAM dané aplikaci - na základě detailní specifikace, řízení a ukládání přístupových oprávnění popř. organizační struktury aplikací, je vytvořeno/nakonfigurováno rozhraní, prostřednictvím kterého IAM aktivně poskytuje data této aplikaci. Data z IAM mohou být poskytována přímo do databázových tabulek dané aplikace, do souborů uložených na disku, do webové služby či jiným podobným způsobem.

(c) řízením aplikace pomocí skupin v AD, IAM v tomto případě pouze zařazuje a vyřazuje uživatele do a z NT skupin.

(d) evidencí oprávnění v aplikaci - v tomto případě řízená aplikace využívá vlastní nástroje pro správu přístupových oprávnění, které jsou zcela nezávislé na IAM, kde jsou pouze evidenčně vedena přidělená přístupová oprávnění za účelem udržení přehledu o přidělených oprávněních jednotlivým uživatelům v rámci celého informačního systému.

(22) Integrační middleware pro komunikaci z ISZR musí tvořit centrální komunikační bod, jehož prostřednictvím musí přistupovat ke službám ISZR jednotlivé součásti (aplikace) informačního systému úřadu. Při každém volání služby integračního middleware ověří tento v IAM oprávnění uživatele přistupovat ke službám ISZR v dané roli. V případě neúspěšného ověření (uživatel nemá oprávnění k dané roli), odmítne integrační middleware tento požadavek ještě před tím, než bude vyvolána komunikace s ISZR.

(23) Komunikační infrastruktura ESB musí umožnit zprostředkování veškeré komunikace mezi součástmi informačního systému úřadu a IAM.

(24) Integrační platforma (ESB) musí být koncipována na principech technologie SOA – Service Oriented Architecture, musí umožňovat integraci na úrovni business procesů tj.

propojování komponent službami. Integrační platforma musí splňovat alespoň následující charakteristiky:

(a) Podpora EAI – Enterprise Application Integration - jedná se o nástroje zajišťující B2B integraci. Umí používat formáty EDI, XML, EDIFACT apod.

(b) Podpora návrhu dynamických distribuovaných obchodních procesů – vizuální vývojové prostředí pro datové procesy v rámci integrace

(c) Prostředí webových služeb pro zajištění integrace – prostředí pro vývoj webových služeb zajišťujících rozhraní pro komunikaci

(d) Definice standardů komunikace – definice standardů dokumentů pro komunikaci, převážně založené na XML formátu

(e) Aplikační adaptéry (vertikální) – spojují integrační broker s vybranou konkrétní aplikací (např. SAP, Siebel, PeopleSoft, Navision, Great Plains).

(f) Technologické adaptéry (horizontální) – spojují integrační broker s okolím prostřednictvím technologie nezávislé na konkrétní aplikaci (např. webové služby, souborový systém, SMTP, TCP/IP, LU 6.2, MQSeries, FTP).

(g) Datové adaptéry – umožňují integračnímu brokeru komunikovat přímo s databází (např. MS SQL, Oracle, DB2).

(25) Integrační sběrnice ESB musí splňovat alespoň následující charakteristiky:

(a) Centralizovaná integrační logika a běhové prostředí

(b) Přesun řešení nekompatibilit mezi systémy na ESB

(c) Dynamické směrovaní dle aktuální situace a požadavků na SLA

(d) Konverze rozdílných přenosových protokolů mezi konzumenty a poskytovateli služeb

(e) Transformace obsahu a datového formátu zpráv mezi konzumenty a poskytovateli služeb

(f) Identifikace a distribuce událostí z rozdílných zdrojů

(g) Zajištění škálovatelnosti a vysoké dostupnosti

(h) Redukce integrační logiky v aplikacích

(i) Redukce počtu a druhů rozhraní na straně aplikací

(j) Zrychlení a zavádění integrace služeb a procesů

(k) Mediační moduly a kompozitní služby

(l) Integrace nových konzumentů služeb bez zásahů do poskytovatelů

(m) Široká podpora standardních komunikačních protokolů a datových formátů (HTTP(S), XML, Webové služby)

(n) Možnosti rozšíření podporované konektivity o aplikační a technologické adaptéry (soubor, email, FTP, atd.) včetně podpory vývoje vlastních adaptérů

(o) Zásadní možnosti v oblastech monitoringu a bezpečnosti

(p) Redukce času potřebného pro integraci služeb prostřednictvím komfortního nástroje pro vývoj integrační logiky, který umožňuje snadnou integraci bez znalosti konkrétního programovacího jazyka či technologie

(26) V rámci dodaného řešení budou vytvořeny minimálně tyto integrační vazby:

(a) Přenos dat z personálního systému FLUX do IAM

(b) Přenos dat z IZSR (RPP) do IAM

(c) Přenos dat z SVI do IAM

(d) Přenos dat na portál úředníka z IAM

(e) Autorizace požadavků na IZSR pomocí IAM

(f) Integrace stávajícího systému SVI a stávajícího systému IS Městské Policie (IS MePol)

(g) Komunikace AIS s ISZR - ESB slouží jako jediný přístupový bod (proxy) pro zabezpečený, logovaný a autorizovaný přístup k základním registrům (ISZR). ESB přebírá požadavek od AIS ve formátu určeném pro komunikaci s ISZR (Webová služba). Požadavek je autorizován IAM, zalogován a odeslán přes firewall a síť KIVS do ISZR. Odpověď ISZR je přijata pomocí ESB a předána na AIS.

(27) Integrační sběrnice ESB musí umožňovat alespoň tyto úrovně integrace aplikací:

(a) Jednoduchá výměna dat mezi aplikacemi

(i) Vyměňovaná data prochází jediným bodem - snadné monitorování výměny dat (centrální log), jsou okamžitě vidět poruchy v komunikaci, zabezpečení (jediné místo, bezpečnostní log)

(ii) Nezávislý arbiter při kolizích - umožňuje určit, na které straně je problém, zabrání výmluvám na "tu druhou aplikaci"

(b) Zpracování procházejících dat

(i) Kontrola procházejících dat - ověření elektronických podpisů, kontrola formální správnosti (datum, číslo...), ověření kontrolních součtů

(ii) Načítání informací z procházejících dat - načtení adresáta a odpovídající směrování, konverze dat do jiného formátu, převod do formátu, který "zná" přijímající aplikace

(c) Procesní zpracování výměny dat

(i) Spojení dílčích integrací do jednoho procesu - definice workflow, zajistí průchod požadovanými kroky, zabrání předčasnému ukončení procesu, krok může znamenat interakci s uživatelem nebo aplikací, vůči uživateli lze použít vygenerovaný elektronický formulář

(ii) Využití informací z procházejících dat - řízení procesu dle načtených dat

(iii) Zápis do procházejících dat - výsledek kroků procesu může být zaznamenán

(d) Měření a monitorování procesů

(i) Dispečink běžících procesů - detekce poruch v reálném čase, umožňuje včas řešit problém

(ii) Analýza ukončených procesů (měření procesu) - nalezení "úzkého hrdla", posílení nejvíce zatížených míst, motivace odpovědných pracovníků, průběh zátěže v čase, posílení kapacit ve špičkách, plánované výpadky při nejmenším provozu, optimalizace, návrh úprav procesu

(28) Integrační sběrnice ESB musí umožňovat šifrování a autentizaci v souladu s průmyslovými standardy, alespoň však XML průmyslové standardy, Kerberos autentizaci i Public Key Infrastructure (PKI). Musí být podporováno zabezpečení síťové komunikace pomocí průmyslových standardů Secure Sockets Layer (SSL) a Transport Layer Security (TLS).

(29) Integrační sběrnice ESB musí umožňovat zabezpečení přihlašování pomocí Enterprise Single Sign-On (SSO).

(30) Integrační sběrnice ESB musí umožňovat zabezpečení SQL Serveru jako úložiště dat (procházejících zpráv, logů atd.), nejvíce citlivé informace, jako přihlašovací údaje, connection stringy apod. musí být uloženy v šifrovaném formátu v Single Sign-On (SSO) databázi.

(31) Zadavatel z důvodu minimalizace rizika neoprávněného přístupu do ISZR, a tím možného úniku informací, požaduje prokázání jakosti dodávaného řešení dle bodu (22) certifikátem vystaveným nezávislým subjektem akreditovaným národním akreditačním orgánem, který má pro dané ověření shody akreditován vhodný postup.

(32) Zadavatel v rámci budování informačních systémů 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.

(33) Servery použité pro realizaci předmětu plnění musí být realizovány jako virtuální se sdíleným datovým úložištěm.

(34) Pokud uchazeč vyžaduje využití konkrétních softwarových řešení a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny. Stejně tak, pokud uchazečem navržená softwarová řešení vyžaduje infrastrukturu neobsaženou v předmětu plnění, zahrne uchazeč do své ceny náklady na její pořízení. Pokud uchazeč vyžaduje nasazení fyzických serverů z důvodů licenčních nebo výkonových, do své ceny zahrne náklady na její pořízení. Zadavatel nedisponuje volnou kapacitou v instalovaných bladových centrech.

(35) Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a technologií v případě, že uchazeč vyžaduje ve svém řešení stejné nebo podobné funkce, jak již poskytují stávající prostředky a technologii. Není přípustné implementovat např. další Active Directory, serverovou virtualizační platformu apod.

(36) Pro předmět plnění bude zabezpečena podpora provozu po dobu 60 měsíců od přechodu systému do plného provozu.

(37) Předmět plnění bude realizován v technologickém centru zadavatele, které se nachází v sídle zadavatele.

3.2. Implementační služby

(1) V rámci realizace předmětu plnění uchazeč realizuje alespoň následující služby:

(a) Provedení předimplementační analýzy. V rámci předimplementační analýzy budou zmapovány alespoň následující oblasti:

(i) životní cyklus uživatelské identity v rámci infrastruktury

(ii) ochranné a kontrolní mechanismy v rámci průběhu životního cyklu uživatelské identity

(iii) vzájemná provázanost jednotlivých systémů ve vztahu k uživatelským identitám a jejich umístění v rámci infrastruktury KV

(iv) nároky infrastruktury na bezpečnost identity v průběhu životního cyklu a komunikace

(v) nároky infrastruktury na autorizaci

(vi) legislativní, procesní a předpisová dokumentace ve vztahu k problematice Identity Managementu

(vii) procesy a agendy úřadu dotčené legislativními požadavky vyplývajícími ze zákona č. 111/2009 Sb., o základních registrech a zákona č. 101/2000 Sb., o ochraně osobních údajů

(viii) požadavky vyplývajících z připojení k Informačnímu systému základních registrů (ISZR)

(ix) určení vazeb mezi aplikacemi a systémy

(x) definice a popis rozhraní potřebných pro integraci

(b) Provedení detailního návrhu cílového stavu, který se bude věnovat mj. i konfiguraci a úpravám systému Identity Managementu, návrhu propojení aplikací pomocí integračního nástroje, možnostem využití bezpečnostního rozhraní pro oblast Identity Managementu a integrace aplikací, zejména v oblasti autentizace a autorizace se snahou o zvýšení stupně poskytované ochrany.

(c) Dodávka a implementace předmětu plnění včetně technické podpory.

(d) Zajištění projektového vedení realizace předmětu plnění

(e) Zpracování prováděcí dokumentace

(f) Zpracování technologické dokumentace (dokumentace skutečného provedení) včetně parametrů a konfigurací – bude vypracována pro každou samostatně upravovatelnou část, bude obsahovat alespoň specifikace řešení (integrace, topologie, atp.) verze jednotlivých produktů, závislosti a vazby, konfigurace

(g) Zpracování provozní dokumentace – bude vypracována pro každou samostatně upravovatelnou část, bude obsahovat alespoň startovací postupy, restartovací a vypínací postupy, základní testy funkčnosti, postupy pro běžný troubleshooting, popis zálohovacích procedur a popis procedur obnovy

(h) Zpracování materiálů pro školení minimálně pro kategorie: uživatelé, administrátoři

(i) Provedení školení v definovaném rozsahu

(j) Provedení akceptačních testů

(k) Zajištění zkušebního provozu v délce minimálně 4 týdnů včetně technické podpory minimálně 2 specialistů na dané zařízení/službu s dostupností maximálně 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h a s průběžným vyhodnocováním minimálně 1x týdně

(l) Předání do plného provozu

(m) Zajištění ostatních služeb potřebných pro realizaci projektu

(2) Uchazeč dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.

(3) Zadavatel požaduje před zahájením implementačních prací zpracování prováděcí dokumentace, která bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění do stávajícího prostředí technologického centra. Prováděcí dokumentace musí být před zahájením prací schválena zadavatelem. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

(a) Komplexní analýzu stávajícího prostředí. Výstupem analýzy bude zejména popis provázanosti identit nebo jejich replikace do ostatních systémů, možnosti autorizačních a autentizačních mechanismů v rámci infrastruktury úřadu, popis politiky, předpisová základna a základní aspekty legislativy, popis pokročilé metody ochrany tak, jak by mohly být v návaznosti na Identity Management dále nasazovány. Dále bude analýza obsahovat alespoň následující:

(i) Seznam rolí v prostředí KV a jejich na mapování na role (skupiny) v personálním systému FLUX

(ii) Definici přenosu identity, jejích rolí a atributů z FLUX do IAM

(iii) Definici procesů v IAM managementu

(iv) Definici přenosu identity, jejich práv a rolí do integrační platformy ESB

(v) Definici přenosu identity, jejich práv a rolí do ostatních vyjmenovaných aplikací

(vi) Popis řešení pro automatizaci procesů spojených s pracovním poměrem, zpracování informačních řezů, proces řízení oprávnění

(vii) Definici zdrojové a cílové podoby datových zpráv přenášených mezi aplikacemi a ESB

(viii) Definici protokolů použitých pro přenos zpráv mezi aplikacemi a ESB

(ix) Definici způsobů autorizace a autentizace při přebírání zpráv mezi aplikacemi a ESB

(x) Definici zabezpečení zpráv (šifrování, podepisování) při předávání mezi aplikacemi a ESB na úrovni zprávy i na úrovni protokolu

(xi) Definici konkrétních adres portů na straně aplikací určených pro přenos zpráv mezi aplikacemi a ESB

(b) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému. Popis bude obsahovat alespoň:

(i) DataFlow Model – cílem je definovat, která data jsou importována do metadirectory a které jsou z něj naopak exportována do jednotlivých připojených datových zdrojů. Definovat datové zdroje a objekty, které budou poskytovat data do metadirectory. Definovat datové zdroje a objekty, které budou využívat data z metadirectory. Definovat charakteristiky dat.

(ii) Koncept DataFlow – DataFlow model je souborem politik a diagramů reprezentující požadavky na návrh, které je nutné do návrhu zahrnout. Koncept je tedy upřesněním politik, které se musí promítnout např. externisté nebudou v databázi FLUX, ale budou mít účet. Definovat základní filtry dataflow do metadirectory. Definovat omezení dataflow - požadavky na unikátnost, požadavky na atributy, validita dat.

(iii) Definice data autorizace – protože stejná data mohou přicházet z různých zdrojů a mohou se v některých atributech lišit je nutné definovat prioritu nebo autoritu jednotlivých datových zdrojů - kdo bude koho oprávněn přepisovat, atributy – nadřazenost, objekty – nadřazenost

(iv) Vytvořit systémové DataFlow - identifikovat skutečné typy identit, identifikovat datové zdroje – definovat typ management agenta

(v) Design metadirectory

(vi) Design synchronizačních pravidel - synchronizační scénáře, seznam pravidel, filtrační pravidla, pravidla mazání, provisioning pravidla, deprovisioning pravidla, dataflow pravidla

(c) Způsob zajištění potřebných dodávek včetně technické podpory

(d) Způsob zajištění projektového řízení na straně uchazeče pro realizaci předmětu plnění

(e) Detailní návrh a popis postupu implementace předmětu plnění

(f) Detailní popis zajištění bezpečnosti informací

(g) Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně tyto aktivity s uvedením konkrétních termínů, uchazeč vhodným způsobem rozšíří kritické milníky o další aktivity, které mohou být pro projekt klíčové. Jedná se o tyto aktivity:

(i) Zahájení projektu

(ii) Provedení předimplementační analýzy

(iii) Předání prováděcí dokumentace

(iv) Zahájení realizace IAM

(v) Zahájení realizace integrační platformy ESB

(vi) Integrace personálního systému FLUX a IAM

(vii) Integrace s ISZR

(viii) Integrace portálu úředníka

(ix) Integrace SVI a IS MePol

(x) Školení

(xi) Zahájení zkušebního provozu

(xii) Akceptační testy

(xiii) Zahájení plného provozu.

(h) Návrh akceptačních kritérií a akceptačních testů

(i) Detailní popis navrhovaných školení

(j) Detailní popis údržby systémů

(k) Obsah provozní dokumentace (technická, uživatelská, administrátorská)

(4) Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem na datovém nosiči a 1x kopii v papírové formě.

3.3. Školení

(1) Uchazeč zajistí školení pracovníků Zadavatele v minimální počtu 10 osob na všechny části systému a problematiku provozu minimálně v rozsahu technologické dokumentace a provozní dokumentace.

(2) Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin – školení bude zakončeno písemnou zkouškou potvrzující požadovanou úroveň znalostí Pracovníků a úspěšným pracovníkům bude vystaveno osvědčení o školení.

(3) Minimální rozsah školení je 24 hodin.

(4) Školení bude probíhat v místě plnění.

4. Záruky a servisní podmínky

(1) Zadavatel požaduje záruku (dále jen „standardní záruka“ nebo jen „záruka“) na veškeré dodané technologie včetně nezbytných provozních a servisních služeb v délce trvání minimálně 12 měsíců od okamžiku ukončení implementace a předání do produkčního provozu. Záruka musí být součástí pořizovací ceny. Veškeré opravy (včetně komponent, náhradních dílů a práce) po dobu záruky budou poskytnuty bezplatně v rámci záruky. Uchazeč ve své nabídce výslovně uvede všechny podmínky standardní záruky.

(2) Zadavatel požaduje v případě hardware provedení záruční opravy do druhého dne nebo poskytnutí náhradního prvku shodných nebo lepších parametrů po dobu opravy. V případě software Zadavatel požaduje provedení záruční opravy formou BE (Best Effort) pokud se jedná o produkt Uchazeče nebo provedení záruční opravy v rámci SLA, kategorie Incident typu D v případě produktu třetí strany.

(3) Zadavatel požaduje rozšířenou záruku (pro software tzv. maintenance), která pokrývá období od konce platnosti standardní záruky do konce doby udržitelnosti. Uchazeč ve své nabídce výslovně uvede všechny podmínky a cenu za rozšířené záruky. Rozšířená záruka musí být součástí ceny za zabezpečení provozu. Veškeré opravy (včetně komponent, náhradních dílů a práce) po dobu rozšířené záruky budou poskytnuty bezplatně v rámci rozšířené záruky.

(4) Po dobu udržitelnosti projektu, tj. 60 měsíců od předání díla jako celku do ostrého provozu, musí dodavatel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu, jako součást garance dodavatel prokáže podporu dodavatele popř. výrobce dodávaných zařízení.

(5) Uchazeč prokáže způsob zajištění shody dodávaných systémů s platnou legislativou.

(6) Uchazeč uvede provozní a servisní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou předmětem dodávek v rámci záruky systému.

5. Požadavky na zabezpečení provozu

Zadavatel požaduje detailní návrh podmínek podpory zajištění provozu, zajišťující garantovanou úroveň služeb podpory zajištění provozu předmětu plnění na dobu 60 měsíců od doby předání do plného provozu. Uchazeč podle svého uvážení může provést úpravu parametrů, pokud takové úpravy nepovedou ke zhoršení podmínek zajištění podpory provozu.

5.1. 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 – standardní 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) **Běžná pracovní doba** – čas mezi 8:00 a 17:00 v Pracovní dny.

(6) **Člověkohodina -** práce Pracovníka Uchazeče v rozsahu jedné (1) hodiny v rámci Pracovního dne.

(7) **Člověkoden -** práce Pracovníka Uchazeče v rozsahu jednoho (1) Pracovního dne.

(8) **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 Dodavatele směřující k odstranění Incidentu, zodpovězení Dotazu nebo přípravy Nového požadavku.

(9) **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

(10) **HelpDesk** – nepřetržitě dostupný automatizovaný systém pro vzdálené zadávání a správu požadavků,

(11) **Hot-line** –pracoviště uchazeče přijímající Požadavky od Zadavatele na definovaných telefonních číslech nebo elektronických komunikačních kanálech.

(12) **Incident** - událost způsobující odchylku od očekávané funkce Prvku IT, která způsobuje nebo může způsobit přerušení anebo snížení kvality této funkce.

(13) **Priorita Incidentu** - závažnost Incidentu dle klasifikace Kontaktní osoby Zadavatele.

(14) **Koncová zařízení** - počítače uživatelů, jejich programové vybavení a periferní zařízení k počítačům připojená (např. tiskárny, skenery).

(15) **Monitorování** - sledování Prvků IT prostředky Vzdáleného přístupu, zda jsou funkční. Sledování, zda provozní charakteristiky Prvků IT nepřesahují stanovené hodnoty, eventuálně neklesají pod stanovené hodnoty. Monitorováním se případně rozumí sledování a archivování jejich provozních charakteristik.

(16) **Proaktivní monitorování** - monitorování prováděné dle charakteru provozu a činnosti Prvku IT v režimu 24x7 (komunikační infrastruktura) nebo v režimu 9x5 (technologické centrum).

(17) **Náhradní zařízení** – zařízení podobných vlastností (parametrů).

(18) **Požadavek** - žádost o provedení Servisní služby na jednom nebo více Prvcích IT.

Požadavek může zahrnovat:

(a) žádost o odstranění závady (nefunkční Prvek IT nebo nesprávná činnost Prvku IT) Incidentu

(b) žádost o poskytnutí konzultace

(c) žádost o provedení Změny

Požadavek může:

(d) být zadán Zadavatelem jako jednorázový

(e) být zadán Zadavatelem jako opakující se činnost

(f) vzniknout jako výstup Monitorování

(g) vzniknout na základě Správy a údržby Prvku IT

(19) **NBD-Next Business Day** – následující pracovní den

(20) **Neprodleně** – bez zbytečného odkladu, s vyvinutím maximálního úsilí na zjednání nápravy nebo zajištění činnosti, nejpozději však následující Pracovní den.

(21) **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.

(22) **Prvek IT** - zařízení (Koncové zařízení, server či jiný hardware), program (software) nebo komunikační linka.

(23) **Rozsah poskytovaných služeb** – specifikace Služby a kvantifikace rozsahu Služby

(24) **Řešitel** - Pracovník Uchazeče, podílející se na řešení Požadavku.

(25) **Report** – přehledový dokument, ve kterém je popsán průběh realizace Plnění za uplynulé období a hodnoty sledovaných parametrů.

(26) **SLA (Service Level Agreement)** - definice kvalitativních parametrů/metrik Služby

(27) **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.

(28) **Služby** – činnosti potřebné pro řádné zabezpečení podpory provozu díla

(29) **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.

(30) **Vzdálená správa** – provádění činností na Prvcích IT, přičemž činnosti nejsou prováděny v místě provozovny Zadavatele, ale prostřednictvím Vzdáleného přístupu z místa provozovny Uchazeče.

(31) **Vzdálený přístup** – připojení z provozovny Uchazeče k zařízení Zadavatele pomocí komunikační linky, na které je vytvořeno dočasné nebo trvalé spojení.

(32) **Zprovoznění náhradním způsobem** - se rozumí zajištění základních funkcí systému, tedy dosažení stavu, kdy není vážně omezena funkčnost informačního systému nebo jeho částí.

(33) **Změna** - změna parametrů Prvku IT nebo instalace, přemístění či odinstalace Prvku IT.

(34) **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.

(35) **Reklamace** - reklamací je nezvyklá událost v Prvku IT v čase záruční doby, která je v rozporu:

(a) se standardní funkčností Prvku IT a tento rozpor je vůči uživatelské dokumentaci produktu,

(b) s funkcionalitou definovanou ve smlouvě (jejích přílohách), případně akceptačním protokolu funkcionality Prvku IT,

(c) s platnou legislativou ČR k datu podání požadavku,

(d) s platnou místní legislativou Zákazníka (vyhlášky, interní normy) k datu podání požadavku.

(36) **Konfigurační management** - jde o službu poskytovanou za účelem udržení aktuální technické dokumentace. V případě jakékoliv provedené změny, bude aktualizována provozní dokumentace o konfiguraci systému včetně zaznamenaných změn. Dokumentace je 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.

(37) **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.

(38) **Hotline podpora** - jde o službu zajišťující poradenství po telefonu nebo elektronické komunikaci

(39) **Maintenance** – jedná se o zajištění nových verzí software, nových verzí firmware, přístupu k technické podpoře výrobce a přístupu k databázi řešených problémů.

(40) **Monitorování** – jedná se o službu nepřetržitého online monitorování systémů s upozorněním na kritické nebo neobvyklé události, upozornění budou automaticky zasílána oprávněným pracovníkům Zadavatele. Součástí služby je vzdálený přístup k aktuálním i historickým údajům o stavu systému. Monitorování je souborem takových opatření, která umožňují v kterémkoli čase znát stav Systému a Systémů třetích stran, minimálně v rozsahu:

(a) monitoring operačních systémů

(b) monitoring sítě a síťových propojení Systému a Systémů třetích stran

(c) monitoring databázových systémů

(d) monitoring diskových polí

(e) monitoring Prvků IT třetích stran, které mohou ovlivňovat chod Systému, pokud jsou tyto Prvky IT součástí Dodávky nebo mohou mít na funkci a/nebo dostupnost Prvku IT negativní vliv způsobující incident kategorie A.

(41) **Profylaxe** - profylaxe zahrnuje aktualizace firmware zařízení, aktualizace administrátorských nástrojů, kontrolu logů, kontrolu vytížení a využití, kontrolu kapacit.

5.2. Specifikace rozsahu poskytované podpory provozu

(1) Základní rozsah systémové podpory v rámci měsíčního paušálu:

(a) Pravidelné servisní prohlídky a revize předepsané výrobci

(b) Řešení Incidentů dle podmínek SLA

(c) Profylaxe minimálně každých 6 měsíců

(d) Hotline podpora v režimu 9x5

(e) Patch management

(f) Odborná podpora v režimu 9x5 – vzdálené konzultace pro dodané služby/produky

(2) Další služby v rámci měsíčního paušálu

(a) Zajištění tj. instalaci a zprovoznění maintenance (nových verzí software a přístup k technické podpoře výrobce) a aktualizací pro veškerý dodaný software

(b) Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.

(c) Legislativní servis

(3) Seznam prvků IT pokrývaných v rámci smlouvy vyplývá ze Zadávací dokumentace a jejích příloh, detailní seznam je součástí Prováděcí dokumentace.

(4) Uchazeč v rámci zpracování Prováděcí dokumentace stanoví kontaktní osoby a způsoby hlášení požadavků minimálně v rozsahu: emailová komunikace, telefonní komunikace, internetová komunikace a podle svého uvážení doplní další možné komunikační kanály pro zabezpečení podpory provozu a technické požadavky na jejich využití. Odpovědné osoby Zadavatele budou stanoveny v průběhu realizace I.etapy tj. Prováděcí dokumentace.

(5) Předmět plnění bude provozován v technologickém centru zadavatele.

5.3. Způsob poskytování plnění

(1) Plnění je poskytováno zejména následujícím způsobem:

(a) Prostřednictvím pracovníka Uchazeče přímo na pracovišti Zadavatele

(b) Prostřednictvím pracovníka Uchazeče Vzdálenou správou

(c) Prostřednictvím pracovníka Uchazeče formou vzdálené konzultace

(d) 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

(a) v případě Monitorování a Vzdálené správy zajistit a udržovat podmínky pro Vzdálený přístup Uchazeče k Prvkům IT.

(b) zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele.

(c) 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.

(d) 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,

(e) umožnit Uchazeči v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu.

(f) 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

(a) písemně či elektronicky potvrdit Uchazeči provedení služby,

(b) 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,

(c) 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.

5.4. 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:

(a) jednoznačná identifikace Požadavku

(b) navrhovaná kategorizace a závažnost,

(c) popis Incidentu nebo Požadavku,

(d) jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh,

(e) kontaktní osoba.

(3) Uchazečem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.

(4) Incidenty musí být 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.

(5) 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.

(6) 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 software 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).

(7) 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.

(8) 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.

(9) 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.

(10) V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:

(a) čase vyřešení požadavku,

(b) v případě Incidentu specifikuje příčinu (pokud je známa),

(c) vyzve iniciátora k ověření funkčnosti služby.

(11) Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.

(12) 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.

(13) 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 ke způsobem řešení nebo výsledném stavu Prvku IT, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

5.5. 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	1 hod	Nejpozději do 12 hod
B	15 min	4 hod	NBD
C	15 min	NBD	5BD
D	15 min	NBD	BE

(2) Zadavatel si vyhrazuje právo udělit Uchazeči smluvní pokutu při nedodržení garantovaných parametrů definovaných v SLA formou poskytnutí slevy ve výši 1 (jedné) měsíční platby.

(3) Zadavatel si vyhrazuje právo navýšit smluvní pokutu v případě opakovaného nedodržení garantovaných parametrů definovaných v SLA v období 6 po sobě následujících měsíců až na 5(pět) měsíčních plateb.

(4) Pro předání požadavků na plnění závazků vyplývajících z SLA je požadováno použití technologie umožňující nepřetržitý dálkový přístup v českém jazyce.

(5) 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.