Příloha č. 1 zadávací dokumentace

Technická specifikace předmětu plnění

Předmětem plnění veřejné zakázky je dodávka a nasazení „Identity management systému" (IDM). IDM umožní automatizovat správu organizačních struktur, systematizovaných míst a účtů (identit) uživatelů. Základním zdrojem dat pro IDM je personální informační systém. IDM bude i nástrojem pro audit oprávnění uživatelů. Z pohledu zadavatele je klíčová vazba systému správy identit na systémy vztažené ke komunikaci se základními registry. IDM musí podporovat správu identit a agendových činnostních rolí pro tyto systémy.

Požadavky na IDM:

- IDM bude udržovat identity a organizační strukturu ve své vnitřní databázi. Identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy.
- IDM bude udržovat a spravovat kompletní životní cyklus identity v počtu minimálně 3000 uživatelů. Zadavatel požaduje licencování formou multilicence bez omezení na počet uživatelů.
- IDM umožní spravovat více organizačních struktur a více organizací.
- IDM umožní definovat a administrovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.
- IDM bude obsahovat samostatný server (Portál) pro přístup koncových uživatelů a samostatný server pro správu a výkon jednotlivých integračních a provozních úloh.
- Identita v IDM musí obsahovat jednoznačný a unikátní identifikátor nezávislý na údajích uživatele. Identifikátor musí být zvolen tak, aby vždy byl jednoznačně spojen s konkrétní fyzickou osobou a aby se neměnil v případě změn souvisejících s touto osobou (např. při změně příjmení, pracovního zařazení a jiné). Údaje k identitě mohou být čerpány z různých informačních systémů.
- IDM musí umožňovat evidenci a správu certifikátů elektronických podpisů pracovníků v souladu s jejich pracovními oprávněními.
- IDM musí implementovat princip založený na systemizovaných místech. IDM musí umožnit systemizaci pracovních míst v souladu se strukturou úřadu, definovat jednotlivá systematizovaná místa a jejich činnosti a sadu oprávnění a rolí pro jednotlivé IS úřadu vztažené ke konkrétnímu systemizovanému místu.
- IDM umožní přiřazení identit na takto vytvořená systematizovaná místa a to i ve vazbě M:N. Identita tedy může být v systému IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.

- IDM musí umožňovat přidělení oprávnění nebo role konkrétní identitě, systemizovanému místu, skupině nebo organizační jednotce.
- IDM musí umožnit autorizaci (ověření oprávnění) uživatelů při přístupu k Informačním systémům úřadu.
- IDM umožní registraci aplikací a jejich rolí. Dále pak import rolí přes webové služby do IDM.
- IDM umožní správu uživatelských rolí, včetně zařazení uživatele do odpovídající role v daném IS.
- IDM bude umožňovat databázovou historizaci.
- V IDM bude možné dynamicky konfigurovat pravidla pro začleňování uživatelů do skupin na základě atributů identity a přidružených referenčních objektů. (organizační jednotka, aplikační role, systematizované místo atd.). Stejným mechanismem pravidel bude možné automaticky vytvářet další účty uživatele. Pravidla bude možné spravovat v grafickém editoru.
- Zadavatel požaduje vytvoření produkčního a testovacího prostředí.
- Zadavatel požaduje řešení postavené na standardizovaném SW produktu . *Za standardizovaný produkt Zadavatel považuje produkt, který je opakovaně implementován (tj. je násobně využíván v rámci autonomních instalací) a existuje síť partnerů výrobce nebo původce SW technologie, kteří produkt technicky podporují.*
- Zadavatel požaduje uvést licence konkrétního produktu, který bude nabízen v rámci řešení.
- Zadavatel požaduje uvést počet licencí konkrétních produktů, které zabezpečí bezproblémový chod nabízeného řešení v souladu s požadavky zadavatele, a to jak v testovacím prostředí, tak produkčním.
- Zadavatel požaduje časově neomezené licenční pokrytí, jak HW, na němž bude řešení provozováno, tak SW.
- IDM bude obsahovat potřebné nástroje a komponenty pro zapojení do architektury federace identit jako poskytovatel identit. Architektura federace identit agreguje více poskytovatelů identit za účelem vytvoření jednotného mechanismu autentizace a autorizace uživatelů pro jednotlivé koncové aplikace a služby.

Požadavky na portál IDM:

- Portál IDM bude webová aplikace přístupná minimálně přes prohlížeče Internet Explorer verze 9 a vyšší, Firefox verze 34.0 a vyšší, Chrome verze 39.0 a vyšší.
- Přístup uživatelů k datům IDM bude zajištěn prostřednictvím webového rozhraní. Řešení musí umožňovat zobrazení přidělených rolí k jednotlivým identitám s rozdělením na role navázané na systemizované místo, na role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu a na role přidělované pro jednotlivé případy. U identity musí být evidován souhrn všech rolí

včetně informace o tom, odkud roli zdědil (z organizační jednotky, systematizovaného místa, skupiny).

- IDM musí umožnit definovat vztahy zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou úřadu mohli delegovat v případě potřeby (dovolená, služební cesta,…) svoje role, nebo jejich část na jiné pověřené osoby a to i tak, že jeden uživatel může mít pro každou svou činnost nastaveného jako zástupce jiného různého uživatele.
- IDM musí umožnit delegování administrátorských práv IDM.
- Portál musí umožnit exportovat a publikovat informace k identitě uložené v IDM a to i historické.
- Webový IDM portál, umožní správu identit uživatelů (interních i externích) a jejich případnou řízenou nebo neřízenou úpravu, založení nebo zneaktivnění/smazání externích identit.
- Portál umožní uživateli měnit některé údaje o své identitě (např. změna hesla).
- Portál umožní grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu bude možné zobrazit organizační strukturu včetně pracovních pozic organizace, až do úrovně jednotlivých uživatelských účtů (identit).
- V portálu bude možné evidovat certifikáty uživatelů a informace o certifikátech. Tyto certifikáty bude rovněž možné nahrávat přes webové služby IDM. IDM bude zneplatňovat automaticky certifikáty, které jsou po vypršení jejich platnosti.
- IDM umožní evidenci následujících samostatných identifikovatelných objektů, na které se identita odkazuje: systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role, certifikát atd.
- IDM umožní přes portál dodatečné přidávání vlastních atributů k identitám a referenčním objektům (viz předchozí bod) a jejich publikaci externím aplikacím přes rozhraní webových služeb.
- IDM umožní správu rolí a oprávnění nezbytných pro komunikaci s RPP (matice agend, činností, systematizovaných míst a osob).
- Veškeré požadavky, které provedou uživatelé na Portálu IDM budou provedeny transakčně. Budou historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách, referenčních objektech, ale i v administraci. Záznam v historii bude obsahovat původní i novou hodnotu.
- IDM umožní definování jednotlivých úrovní administrátorských oprávnění k identitám a stromové struktuře. V IDM musí být zejména možnost vytvářet administrátorské role na úrovni jednotlivých organizačních jednotek jako přiřazovatel vybraných aplikačních rolí (pro organizační jednotku), činnostních rolí a správce identit.

- IDM bude umožňovat generovat auditní reporty v XML – zobrazení daného uživatele a jeho rolí v IS napojených na IDM, agendových rolí, přiřazených skupin ve vybraném časovém okamžiku.
- Přes IDM portál bude možné k účtům přikládat fotografie.
- IDM bude umožňovat přesun identity mezi jednotlivými organizacemi.
- IDM bude umožňovat kopírovat agendové činnostní role mezi jednotlivými systematizovanými místy
- IDM umožní přes webový portál nastavení, které zabrání hromadným změnám z důvodu případných chybných dat na vstupu (například z personálního systému), tak aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory).
- Synchronizaci bude možné spouštět přes portál ručně i automaticky. Synchronizaci bude možné spouštět i v simulačním režimu, tak aby bylo možné si ověřit stav dopadu reálného spuštění předem. Simulační logy budou k dispozici opět v uživatelském rozhraní portálu IDM.
- IDM umožní upozorňovat na chybové stavy synchronizace pomocí mailu na administrátory IDM a zapisovat je do aplikačního logu na serveru i do interního logu IDM přístupného z portálu IDM.
- Portál IDM umožní sledovat administrátorovi jednotlivé stavy v průběhu synchronizace v grafické podobě.
- Vedle systémové konfigurace IDM bude možné v portálu spravovat synchronizace včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací bude rovněž požadováno, aby bylo možné v IDM vybírat organizace, které se mají z IDM synchronizovat s danými systémy.
- IDM umožní notifikovat emailovou zprávou vytvoření a změny identity.
- IDM umožní notifikovat emailovou zprávou vytvoření a změny referenčních objektů jako systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role atd.
- Mechanismus správy notifikací včetně náhledu na odeslané notifikace bude přímo v portálu IDM.
- V portálu bude možné v šabloně notifikace definovat příjemce, předmět a obsah dané notifikace. U notifikací vázané k identitám bude dále možné nastavovat pro odesílání notifikací samostatné příjemce pro různé části organizační struktury (oddělení, odbory).
- IDM bude podporovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci bude možné nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu.

- Notifikace bude možné aktivovat pro jednotlivé zdrojové systémy, které v IDM změnu identity nebo referenčního objektu provedli. Jedná se například o personální systém, Portál IDM atd.
- IDM bude obsahovat notifikační konektor, který bude simulovat napojení aplikace, která zatím není napojena na IDM. Pokud administrátor IDM nebo automatické pravidlo přidá, odebere identitě roli z této aplikace nebo změní identitu, pošle se emailová notifikace definovanému příjemci (administrátorovi) aplikace.

Požadavky na integraci

Webové služby IDM

- IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů. Základní konfigurace přístupu k webovým službám bude přístupná v portálu IDM.
- Rozhraní bude poskytovat minimálně následující služby
    - Získání organizační struktury
    - Získání hierarchie systematizovaných míst
    - Získání seznamu identit
    - Získání nadřízené osoby pro daného zaměstnance
    - Získání seznamu aplikační 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
    - Služba pro autorizaci pro ISZR – služba ověří validnost volání služby ISZR. Služba bude ověřovat v IDM:
        - Zda je evidován uživatel v IDM, který je požadavku na ISZR
        - Zda je evidována aplikace v IDM, která je požadavku na ISZR
        - 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 IZSR, v IDM povolenou agendovou činnostní roli a agendu, které jsou rovněž uvedeny v požadavku na ISZR.

Napojení na Active Directory

- IDM umožní správu účtu a jejich certifikátů v Active Directory včetně iniciačního načtení účtů z AD.
- IDM umožní správu skupin a členství ve skupinách v Active Directory, včetně iniciačního načtení z AD.
- IDM umožní správu organizačních jednotek v Active Directory včetně iniciačního načtení z AD.
- Zadavatel požaduje, aby součástí plnění veřejné zakázky bylo vybudování samostatného Active Directory pro externí uživatele včetně licenčního pokrytí. IDM bude realizovat správu účtů, skupin a organizačních jednotek i v tomto AD.

Napojení na personální systém

- IDM umožní napojení na personální systém pro získávání organizační struktury, hierarchie systematizovaných míst a osob.

Napojení na RPP

- IDM musí obsahovat evidenci matice práv a rolí dle Informačního systému základních registrů (ISZR-RPP) matice RPP tak, aby vedoucí pracovníci měli možnost zadávat k jednotlivým činnostem konkrétní uživatele (systemizovaná místa) a tyto změny po odsouhlasení odeslat do ISZR-RPP.
- IDM bude umožňovat přidělování/odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systemizovaná místa.
- V IDM bude udržován přehled o oznámené působnosti, jejich stavů, kontrola přeregistrace a změn.
- IDM musí obsahovat evidenci přehledu legislativy včetně vazby na jednotlivé činnosti/agendy. Automatická synchronizace všech požadovaných dat mezi RPP, JIP, IDM.
- IDM umožní inicializační synchronizace IDM, JIP, Personálního systému

Napojení na Ginis

- Data spravovaná v IDM budou pravidelně synchronizována do cílového systému Ginis
- Zdrojem pro získání aplikačních rolí aplikace Ginis do IDM budou konfigurační skupiny evidované v systému Ginis. Pro načtení těchto rolí bude sloužit synchronizace z Ginis do IDM.
- Z IDM budou do systému Ginis pravidelně synchronizovány organizační jednotky, uživatelé, agendy, agendové činnostní role, systematizovaná místa s vazbou na agendové činnostní role a konfigurační skupiny.

- Před spuštěním pravidelné synchronizace organizační struktury do aplikace Ginis budou iniciační synchronizací pro již existující organizační jednotky, systematizovaná místa a uživatele v aplikaci Ginis naimportovány do IDM identifikátory přidělené aplikací Ginis. Tyto identifikátory bude IDM využívat pro další komunikaci se systémem Ginis. Iniciační synchronizaci bude možné spouštět opakovaně. Iniciační synchronizace rovněž nahraje do IDM vazby systematizovaných míst na konfigurační skupiny a agendové činnostní role ze systému Ginis.
- Do systému Ginis budou přenášeni uživatelé, kteří mají přiřazenou roli aplikace Ginis.

Napojení na KDS

- Data spravovaná v IDM budou pravidelně synchronizována do cílového systému KDS
- Zdrojem pro získání aplikačních rolí aplikace KDS do IDM budou konfigurační skupiny evidované v systému KDS. Pro načtení těchto rolí bude sloužit synchronizace z KDS do IDM.
- Z IDM budou do systému KDS pravidelně synchronizovány organizační jednotky, uživatelé, systematizovaná místa s vazbou na konfigurační skupiny.
- Před spuštěním pravidelné synchronizace organizační struktury do aplikace KDS budou iniciační synchronizací pro již existující organizační jednotky, systematizovaná místa a uživatele v aplikaci KDS naimportovány do IDM identifikátory přidělené aplikací KDS. Tyto identifikátory bude IDM využívat pro další komunikaci se systémem KDS. Iniciační synchronizaci bude možné spouštět opakovaně. Iniciační synchronizace rovněž nahraje do IDM vazby systematizovaných míst na konfigurační skupiny a agendové činnostní role ze systému KDS.
- Do systému KDS budou přenášeni uživatelé, kteří mají přiřazenou roli aplikace KDS.

Napojení na KDR

- Data spravovaná v IDM budou pravidelně synchronizována do cílového systému KDR
- Zdrojem pro získání aplikačních rolí aplikace KDR do IDM budou konfigurační skupiny evidované v systému KDR. Pro načtení těchto rolí bude sloužit synchronizace z KDR do IDM.
- Z IDM budou do systému KDR pravidelně synchronizovány organizační jednotky, uživatelé, systematizovaná místa s vazbou na konfigurační skupiny.
- Před spuštěním pravidelné synchronizace organizační struktury do aplikace KDR budou iniciační synchronizací pro již existující organizační jednotky, systematizovaná místa a uživatele v aplikaci KDR naimportovány do IDM

identifikátory přidělené aplikací KDR. Tyto identifikátory bude IDM využívat pro další komunikaci se systémem KDR. Iniciační synchronizaci bude možné spouštět opakovaně. Iniciační synchronizace rovněž nahraje do IDM vazby systematizovaných míst na konfigurační skupiny a agendové činnostní role ze systému KDR.

- Do systému KDR budou přenášeni uživatelé, kteří mají přiřazenou roli aplikace KDR.

Napojení na JIP

- IDM musí umožnit obousměrnou synchronizaci s JIP.
- Z JIP budou do IDM pravidelně načítány jednotlivé aplikace a role.
- Ze strany IDM budou do JIP předávány identity včetně vazby na jednotlivé aplikační a agendové činnostní role.
- Přes portál IDM bude možné měnit heslo uživatele v JIP.

Napojení na Kukátko

- IDM musí umožnit obousměrnou synchronizaci s aplikací Kukátko.
- Z aplikace Kukátko budou do IDM pravidelně načítány aplikační role aplikace Kukátko.
- V IDM bude následně možné tyto aplikační role přiřazovat na jednotlivá systematizovaná místa.
- Ze strany IDM budou do aplikace Kukátko předávány identity včetně vazby na jednotlivé aplikační a agendové činnostní role.
- Ze strany IDM bude do aplikace Kukátko předávána hierarchie systematizovaných míst.

Obecné požadavky pro napojení

- Veškerá napojení na uvedené systémy výše budou řešena režimem synchronizací s požadovanými vlastnostmi:
    - Bude implementována plná a změnová synchronizace za předpokladu, že synchronizovaný systém oba režimy podporuje.
    - U synchronizace bude možné nastavit limit ve formě počtu změn, které je možné zpracovat.
    - U synchronizace bude možné nastavit časový interval automatického spouštění.
    - U synchronizace bude možné nastavit interval odstávky.
    - Synchronizaci bude možné spustit i pouze v simulačním režimu.
    - Synchronizace bude možné spustit ručně.

MS PKI

- IDM bude umožňovat správu certifikátů s vazbou na certifikační autoritu

- IDM musí být schopen evidovat a spravovat certifikáty elektronických podpisů pracovníků MMB v souladu s jejich pracovními oprávněními. Spravovat seznam osob a jejich nastavení (pravidel)

Sharepoint

- IDM bude spravovat identity a oprávnění v platformě Sharepoint
- IDM bude do workflow na Sharepoint předávat informace o nadřízenosti a podřízenosti daných zaměstnanců
- IDM bude do Sharepoint předávat informace o organizační struktuře a kontaktní údaje o zaměstnancích

Datový sklad

- IDM bude spravovat identity a oprávnění pro aplikaci Datový sklad

T-WIST

- IDM bude spravovat identity a oprávnění pro aplikaci T-WIST

VITA

- IDM bude spravovat identity a oprávnění pro aplikaci VITA

EVI

- IDM bude spravovat identity a oprávnění pro aplikaci EVI

ESPI

- IDM bude spravovat identity a oprávnění pro aplikaci ESPI

Požadavky na HW

Součásti implementace IDM je i dodání odpovídající HW infrastruktury (včetně odpovídajících licencí) potřebné pro vybudování produkčního a testovacího prostředí.

Minimální požadavky na infrastruktury jsou uvedeny níže – viz technická infrastruktura.

Technická infrastruktura:

Technická infrastruktura musí zajistit spolehlivé a výkonově dostatečně dimenzované prostředí pro provoz softwarového řešení IdM. Pro spolupráci se stávajícími systémy a pro snadnou správu a údržbu musí být navržené řešení kompatibilní na úrovni managementu a používaných funkcionalit se současnou serverovou a síťovou infrastrukturou MMB (viz níže v tabulkách).

Kapacita prostředků musí být dostatečná pro chod produkční a testovací části nabízeného řešení.

V následujících tabulkách jsou specifikovány požadavky pro jednotlivé prvky technické infrastruktury nutné pro zavedení systému IdM.

Servery 2 kusy: (požadavky jsou specifikovány pro každý kus)

Parametr	Popis
Procesor	Každý server musí mít výkon odpovídající min. hodnotě 3 879 bodů dle https://www.cpubenchmark.net/.
Operační paměť	Min. 48 GB, funkční na min. 1333 MHz v nabízené konfiguraci
Konektivita	LAN min. 2x 1 Gb, SAN min. 2x 8Gb. Včetně potřebných kabelů v délce min 3 m.
Úložiště	Flash úložiště pro provoz hypervizoru VMware ESX
Provedení	Server do racku, výška 1U, včetně montážních prvků a spojovacího materiálu
Management	Integrované řešení pro vzdálenou správu přes LAN, kompatibilní se standardem IPMI v2. Vestavěná diagnostika umožňující určit vadný komponent. Kompatibilita s IBM Systems Director
Záruka, servis	Min. 60 měsíců, oprava následující pracovní den v místě instalace

Tabulka 1 - Specifikace serverů

Síťové prvky 2 kusy: (požadavky jsou specifikovány pro každý kus)

Parametr	Popis
Konektivita	Min. 24x 1Gb RJ-45, 4x 1 Gb SFP
Výkon	Propustnost min. 80 Gb/s L3 a 180 Gb/s na L2 vrstvě
Kompatibilita	Funkční kompatibilita se stávající síťovou infrastrukturou, min. na úrovní VLAN (automatická propagace, 802.1X, agregace portů
Škálovatelnost	Možnost rozšíření pro zahrnutí do stacku kompatibilní s Cisco FlexStack Stacking

Parametr	Popis
Management	Kompatibilita se stávající síťovou infrastrukturou min. na úrovní SNMP (použití stávajících MIB tabulek)
Záruka, servis	Min. 60 měsíců

Tabulka 2 - Síťové prvky

Virtualizace pro 2 servery: (požadavky jsou specifikovány pro každý kus)

Parametr	Popis
Funkčnost	Virtualizační software pro nabízené servery, kompatibilní se stávající virtualizační platformou VMware ESX. Schopnost migrace virtuálních serverů bez přerušení chodu. Vysoká dostupnost – automatické spuštění virtuálního serveru na jiném virtualizačnímhostu v případě poruchy
Licencování	Licence pro oba nabízené servery
Management	Kompatibilita se stávajícím managementem VMware center
Podpora, maintenance	Podpora výrobce a nárok (v ceně) na nové verze software po dobu 60 měsíců

Tabulka 3 - Virtualizace

Operační systémy pro 2 servery: (požadavky jsou specifikovány pro každý kus)

Parametr	Popis

Parametr	Popis
Funkčnost	Možnost adresářové služby kompatibilní s X.509 - Autentizace protokoly Kerberos V5, NTLMv2, NTLM Centrálně řízené politiky uživatelů a počítačů Možnost funkcí DNS, DHCP, WINS. Služba DNS poskytuje mechanismus multimaster replikace Integrovaný webový server s podporou neomezeného počtou domén Možnost sdílení souborů a nastavování práv na objekty adresářové služby Sdílení souborů pomocí protokolu CIFS Distribuovaný souborový systém a delta replikace Možnost sdílení tiskáren a nastavování práv na objekty adresářové služby Možnost grafického uživatelského rozhraní v češtině Podpora technologie .NET Framework v aktuální verzi
Licencování	Licence pro běh min. 8 virtuálních instancí nabízeného operačního systému na každém nabízeném serveru
Podpora, maintenance	Nárok na bezpečnostní aktualizace a opravné patche po dobu 60 měsíců

Tabulka 4 - Operační systémy

Ostatní požadavky

- Záruka 60 měsíců (po uplynutí 60 měsíců dojde k úpravě smlouvy v této oblasti plnění na dobu neurčitou)
- Další technické požadavky
  Předmět plnění veřejné zakázky bude možné nativně provozovat na všech typech níže uvedeného vybavení:
  - prostředí virtuálních serverů VMWare,
  - typ databáze: MS SQL – zadavatel vlastní potřebné licence
  - Internet Explorer, Mozilla Firefox, Google Chrome
  - Součástí nabídky bude položkový rozpočet veškerých potřebných komponent, licencí potřebných pro kompletní implementaci požadovaného řešení.

- Všechny části řešení, které budou v interakci s běžným uživatelem, musí být plně lokalizovány do českého jazyka. U ostatních částí řešení se kromě českého jazyka připouští i možnost anglického jazyka.

Předimplementační analýza

Analýza musí obsahovat minimálně:

- analýzu procesů a aplikací MMB se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí
- analýzu požadavků vyplývající z připojování MMB k centrálním informačním systémům, základním registrům a dalších informačních systémů s požadavkem na autorizaci a autentizaci
- analýzu možností správy výstupních struktur – evidenční údaje, logy.
- analýzu nutných reportů
- návrh životního cyklu Identity uživatelů
- model struktury úřadu
- seznam systemizovaných pracovních pozic
- přiřazení pracovníků k pracovním pozicím
- atributy dodávané personálním systémem v souladu s potřebami obsluhovaných systémů

Návrh řešení cílové architektury IDM včetně vazeb na infrastrukturu (ve formě implementačního projektu)

Implementační projekt bude obsahovat minimálně:

- manažerský souhrn
- analýza výchozího stavu informačního systému – technologický popis stávajících technologií
- detailní popis řešení
- návrh podrobného postupu implementace nabízeného řešení
- harmonogram implementace řešení a realizace celého projektu
- požadavky na součinnost zadavatele (max. 15 MD – dáno plánovanými kapacitami zadavatele na projekt)
- zabezpečení bezpečného přístupů externích uživatelů
- návrh akceptačního protokolu
- přiřazení informačních systémů a oprávnění v nich k jednotlivým činnostem
- přiřazení činností k pracovním pozicím v organizační struktuře
- analýza a soupis požadavků na navrhované řešení a způsob jejich pokrytí
- návrh metodiky pro správu identit a jejich oprávnění
  návrh způsobu udržování historické organizační struktury

Dokumentace

Zadavatel požaduje vytvoření kompletní technické a uživatelské dokumentace odpovídající požadavkům na dokumentaci ISVS podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a souvisejícím právním předpisům (musí splnit požadavky ISMS – normy ISO 27001 na dokumentaci z pohledu řízení informační bezpečnosti). Dokumentace bude jednoznačně a detailně popisovat celé implementované řešení včetně popisu všech rozhraní. Umožní uživatelům na všech úrovních bezproblémovou orientaci v implementovaném prostředí. Technická dokumentace bude mimo jiné obsahovat i popis procesu zálohování a obnovy, monitoringu a procedur bezpečného vypnutí a spouštění systému. Součástí bude nejen dokumentace implementovaného řešení, ale i dokumentace jednotlivých dodaných systémů.

Technické a uživatelské dokumentace bude zadavateli předání v elektronické podobě a ve 2 ks listinných vyhotovení.

Licence

Zadavatel požaduje, aby součástí plnění byly všechny potřebné licence pro provoz dodávaného řešení. Nabídka musí obsahovat všechny potřebné licence aplikací a další potřebný SW a HW související s provozem dodávaného řešení.

Akceptační testy

Předání a převzetí díla bude provedeno na základě protokolu o provedených akceptačních testech. Ukončení akceptačních testů budu stvrzeno podepsáním akceptačního protokolu po ukončení zkušebního provozu. Návrh akceptačních kritérií a obsah a forma akceptačního protokolu bude součástí analýzy a podléhá schválení zadavatelem (zadavatel musí odsouhlasit, které procesy správy identit uživatele budou součástí akceptačního testu). Součástí akceptačních testů musí být minimálně:

- ověření funkčnosti řešení v plném rozsahu technické specifikace
- ověření funkčního řešení v rámci testovacího provozu
- ověření funkčnosti rozhraní pro jednotlivé připojené systémy s důrazem na klíčové IS v požadavcích
- úplná technická a uživatelská dokumentace implementovaného řešení včetně popisu rozhraní pro jednotlivé přípojné systémy

Zkušební provoz

Zkušebním provozem se rozumí doba určená k ověření požadovaných funkcí jednotlivých informačních systémů. Doba zkušebního provozu začíná běžet dnem protokolárního ukončení implementovaného plnění a jeho předání do zkušebního provozu. Délka trvání zkušebního provozu bude 15 dní. Pokud dojde v průběhu zkušebního provozu k závadám, doba zkušebního provozu se prodlužuje o stejnou dobu, po kterou nebyly informační systémy plně funkční.

Zkušební provoz bude ukončen protokolárním ukončením zkušebního provozu a předáním jednotlivých informačních systémů do rutinního provozu na základě podpisu Protokolu o závěrečné akceptaci.

Požadavky na seznámení zadavatele s obsluhou:

V rámci projektu (veřejné zakázky) bude provedeno seznámení administrátorů systému a vybraných uživatelů (správců oprávnění) s obsluhou. Zhotovitel vytvoří osnovy a obsah seznámení uživatelů a správců s obsluhou díla pro jeho kompletní využití.
Seznámení administrátorů systému s obsluhou bude min. v rozsahu čtyř školících dní (8 vyučovacích hodin/den) určeným zaměstnancům zadavatele – správcům systému (max. v rozsahu 5 zaměstnanců) na administraci systému v sídle zadavatele.

Technická podpora

Zadavatel požaduje, aby součástí dodávaného řešení byla min. 5 letá podpora na SW a HW vybavení všech dodávaných komponent (počínaje od akceptace plnění zadavatelem). Podpora bude také zahrnovat provádění změn vyplývajících z legislativních úprav, připojování dalších informačních systémů a agend, ladění a optimalizace řešení.

Servisní parametry SLA musí zahrnovat obnovení provozu v režimu 5/10, v návrhu musí být využito principů HA (High Availability). Zhotovitel je povinen zajistit, aby celková úroveň SLA nebyla nižší než 96 % za kalendářní měsíc.

Postup reakce na závadu/incident zadavatel požaduje takto:

Priorita	doba odezvy	doba odstranění
a) Kritická závažnost	1 hod	6 hod
b) Střední závažnost	2 hod	1 prac. den
c) Minimální závažnost	8 hod	5 prac. dnů

Definice závažností bude vycházet z ČSN EN ISO 20000:2014.

Zadavatel bude požadavky na Technickou podporu provádět prostřednictvím Service Desk (dále jen „*hlášení problému*“). Hlášení problému bude specifikovat předmětnou vadu či incident, postup jak lze problém reprodukovat, požadovanou funkčnost nebo činnost Zhotovitele a kategorii závažnosti problému.

Poskytovatel je povinen potvrdit zahájení řešení hlášeného problému prostřednictvím Service Desk a dále pro případy s prioritou ad a) telefonicky kontaktovat kontaktní osobu zadavatele (Objednatele).

Ing. Jaromír Emmer

Digitálně podepsal Ing. Jaromír Emmer
DN: c=CZ, o=Statutární město Brno, Magistrát města Brna [IČ 44992785], ou=OMI MMB, ou=272600, cn=Ing. Jaromír Emmer, serialNumber=P93150, title=vedoucí odboru
Datum: 2015.03.25 08:20:18 +01'00'