logo szif

**PŘÍLOHA Č. 9**

**zadávací dokumentace k veřejné zakázce  
„Pořízení a implementace systému pro správu identit v IS SZIF“**

**Specifikace předmětu plnění – minimální technické podmínky**

|  |
| --- |
| **Specifikace předmětu plnění – Minimální technické podmínky** |

Níže uvedené minimální technické podmínky stanovuje Zadavatel v rámci veřejné zakázky s názvem „Pořízení a implementace systému pro správu identit v IS SZIF“ za účelem prokázání technických parametrů a vlastností poptávaného systému a schopností samotného nástroje pro správu identit splnit výkonnostní podmínky v prostředí Zadavatele.

S ohledem na klíčovou roli poptávané technologie v informačním systému Zadavatele (informační systém slouží k administraci dotačních titulů v objemu cca 40 mld. Kč ročně), vyžaduje Zadavatel, aby splnění výkonnostních parametrů bylo doloženo produktivně realizovanými a implementovanými projekty prokazujícími výkonnostní parametry samotného nabízeného nástroje a schopnost technologie obsluhovat identity v informačním systému Zadavatele.

## Požadované výkonnostní parametry IDM nástroje

1. Systém IDM je technologicky dimenzovaný pro běžné rutinní užívání v prostředí informačního systému s připravenou integrací na platformu SAP a umožňuje v informačních systémech na platformě SAP plně řídit komplexní správu různých skupin uživatelů včetně jejich přístupových oprávnění a rolí, a to v následujícím rozsahu:

* Správa více než 1500 interních zaměstnanců (identit) v rozsahu uživatelské jméno, heslo, další volitelné a definovatelné atributy (organizační struktura a přiřazení, atributy zaměstnance používané standardně v adresářové struktuře);
* Správa více než 100.000 internetových (portálových, či jinak externích uživatelů), jejichž údaje jsou evidovány v CRM nástroji (jakákoliv platforma) s integrací na prostředí SAP;
* V systémech SAP je možné řízení uživatelských oprávnění a rolí v následujícím objemu:
  + Počet rolí v SAP java systémech (např. SAP NetWeaver Portal) – více než 1500 rolí
  + Počet rolí v SAP R/3 modulech – více než 10.000 rolí;
* Součástí produktivního fungování IDM nástroje je provádění auditních analýz, SoD na úrovni:
  + SAP role,
  + SAP profil,
  + Objekt oprávnění v SAP,

kdy součástí prostředí v informačním systému na platformě SAP jsou uživatelsky (zákaznickým vývojem) vytvořené elementy (role, profil, objekt);

* Správa organizačních struktur v IDM nástroji s integrací na prostředí SAP, kdy součástí správy v nástroji IDM je možnost udržovat různé typy organizačních struktur (organizační struktura společnosti, organizační struktury ad hoc projektů, projektových i provozních týmů, technické organizační struktury s čistě manuální definicí hierarchie), včetně libovolného naplnění jednotlivých typů organizačních struktur uživateli;
* Integrace na prostředí SAP je možná standardními prostředky na centrální správu uživatelů SAP, případně prostřednictvím zákaznicky customizovatelných webových služeb.

**Dodavatel předloží v předběžné nabídce a nabídce písemné potvrzení, z něhož bude jednoznačně vyplývat, že existuje alespoň 1 produktivně a rutinně užívaná instalace IDM nástroje, který splňuje všechny výše uvedené výkonnostní parametry, a že komplexní správa identit a uživatelů byla realizována interně (nikoliv dodavatelsky) s délkou produktivního provozu minimálně 12 měsíců. Toto potvrzení bude vystaveno výrobcem SW nebo objednatelem IDM nástroje.**

1. Systém IDM je aplikačně připravený (bez customizací realizovaných nad rámec standardní instalace a podpory) na integraci na správu uživatelských účtů s adresářovou strukturou a Microsoft Active Directory (MS AD) v následujícím objemu:

* Více než 1500 identit spravovaných prostřednictvím MS AD, kdy primárním zdrojem dat pro MS AD je IDM nástroj;
* Instalace MS AD, na kterou je IDM nástroj integrován, je standardní v souladu s pokyny výrobce bez vytvořených customizací a úprav;
* Prostřednictvím nástroje Identity managementu jsou řízeny účty včetně doménových a administrátorských, které mají odlišný způsob administrace od standardních uživatelských účtů.

**Dodavatel předloží v předběžné nabídce a nabídce písemné potvrzení, z něhož bude jednoznačně vyplývat, že existuje alespoň 1 produktivně a rutinně užívaná instalace IDM nástroje, který splňuje všechny výše uvedené výkonnostní parametry, a že komplexní správa identit a uživatelů byla realizována interně (nikoliv dodavatelsky) s délkou produktivního provozu minimálně 12 měsíců. Toto potvrzení bude vystaveno výrobcem SW nebo objednatelem IDM nástroje.**

1. Systém IDM je aplikačně připraven na integraci s HR informační systémy v následujícím rozsahu:

* V HR systému je evidováno alespoň 1500 zaměstnaneckých identit (jedineční uživatelé);
* Integrace musí být možná na HR nástroje různých výrobců;
* Správa uživatelů je tak možná vícekrokově, kdy primárním zdrojem dat o zaměstnancích je HR systém, ze kterého jsou údaje o zaměstnancích (jméno, příjmení, pozice, identifikátor zaměstnance, organizační přiřazení, další osobní údaje definující zaměstnance) přenášeny do IDM nástroje;
* V IDM nástroji je následně automaticky vytvářena identita zaměstnance;
* K dané identitě je možné vytvářet různé typy uživatelských účtů, kdy pro vytvoření uživatelského účtu je možné uživatelsky správcem IDM nástroje definovat pravidla a politiky stanovující vlastnosti konkrétního typu uživatelského účtu.

**Dodavatel předloží v předběžné nabídce a nabídce písemné potvrzení, z něhož bude jednoznačně vyplývat, že existuje alespoň 1 produktivně a rutinně užívaná instalace IDM nástroje, který splňuje všechny výše uvedené výkonnostní parametry, a že komplexní správa identit a uživatelů byla realizována interně (nikoliv dodavatelsky) s délkou produktivního provozu minimálně 12 měsíců. Toto potvrzení bude vystaveno výrobcem SW nebo objednatelem IDM nástroje.**

## Požadované funkční vlastnosti IDM nástroje

Zadavatel níže uvádí specifické funkční vlastnosti, které vyžaduje jako standardní vlastnost systému IDM technologie. Pokud není uvedeno jinak, jedná se tedy o obecnou vlastnost dostupnou po instalaci, nikoliv funkcionalitu, kterou lze získat specifickým vývojem, případně customizací nástroje.

**Dodavatel doloží splnění funkčních vlastností IDM nástroje tak, že v předběžné nabídce a nabídce předloží technickou (případně uživatelskou) dokumentaci výrobce SW a vyplněnou níže uvedenou tabulku, kdy pro každou z vlastností dodavatel v níže uvedené tabulce uvede odkaz na konkrétní znění dokumentace (strana, odstavec), tak aby bylo jednoznačně prokázáno splnění požadavku.**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Kategorie** | **Požadavek** | **Odkaz na dokumentaci** |
| 1 | Funkcionalita | Systém umožňuje práci minimálně s 5 nezávislými úrovněmi (typy) identit, kdy pro každou úroveň (typ) lze stanovovat vlastní politiky/pravidla/vlastnosti | „Doplní dodavatel“ |
| 2 | Funkcionalita | Pro každý typ identit lze definovat datové struktury (atributy) identit s vlastními vlastnostmi (např. jmenná konvence user name, kontrola dané hodnoty, atd.) | „Doplní dodavatel“ |
| 3 | Funkcionalita | Řešení umožňuje přidělování, odebrání, reorganizaci a modelování rolí (na úrovni business rolí) | „Doplní dodavatel“ |
| 4 | Funkcionalita | Systém umožňuje ohodnocení objektů (atributů, povolení) na základě analýzy rizik | „Doplní dodavatel“ |
| 5 | Funkcionalita | Systém umožňuje grafické zobrazení přístupových práv jednotlivých uživatelů v interaktivní mapě, která zobrazuje i návrhy možných rolí | „Doplní dodavatel“ |
| 6 | Funkcionalita | Systém umožní revizi přístupů a jejich certifikaci včetně zneplatnění | „Doplní dodavatel“ |
| 7 | Funkcionalita | Umožňuje konfiguraci a validaci politik minimálních privilegií | „Doplní dodavatel“ |
| 8 | Funkcionalita | Umožňuje konfiguraci a validaci SoD - Separation of Duties | „Doplní dodavatel“ |
| 9 | Funkcionalita | V systému musí být možno vytvořit vlastní struktury organizace, které reflektují skutečnost. (např.: rozdělení mezi regiony, interní členění, různé organizační struktury, partneři) | „Doplní dodavatel“ |
| 10 | Funkcionalita | Systém umožňuje založení, změnu, dočasné i trvalé zneplatnění, vymazání uživatele | „Doplní dodavatel“ |
| 11 | Funkcionalita | Možnost definovat vlastní politiky provisioningu identit a rolí, hesel a tvorby identit | „Doplní dodavatel“ |
| 12 | Funkcionalita | Systém dokáže identifikovat nepoužívané účty | „Doplní dodavatel“ |
| 13 | Funkcionalita | Systém rozlišuje systémové a technické účty od uživatelských účtů | „Doplní dodavatel“ |
| 14 | Funkcionalita | Systém musí umožňovat definování statických a dynamických rolí, které jsou přiřazovány na základě atributů uživatele | „Doplní dodavatel“ |
| 15 | Funkcionalita | Systém musí umožňovat pokročilou administraci rolí v rámci základní licence (tvorba "what-if" analýz) | „Doplní dodavatel“ |
| 16 | Funkcionalita | Musí umožňovat více­úrovňové schvalovací procesy (workflow) pro správu rolí, oprávnění i samotného řízení identit | „Doplní dodavatel“ |
| 17 | Funkcionalita | Obsahuje nástroje pro modelování workflows včetně vizualizace a umožňuje definování workflows bez nutnosti znalosti programovacích jazyků | „Doplní dodavatel“ |
| 18 | Funkcionalita | Musí umět pracovat s vlastními uživatelsky definovanými atributy včetně jejich správy a nástroji pro modelování rolí | „Doplní dodavatel“ |
| 19 | Funkcionalita | Systém musí být schopen zabránit přidělení oprávnění/role/přístupu pokud by mělo dojít ke střetu zájmů (SoD - Separation of Duties) | „Doplní dodavatel“ |
| 20 | Funkcionalita | Musí umožňovat delegace pravomocí | „Doplní dodavatel“ |
| 21 | Funkcionalita | Podporuje přidělování oprávnění na základě rolí, nebo na základě požadavků, případně kombinací obojího | „Doplní dodavatel“ |
| 22 | Funkcionalita | Možnost pokročilého vyhledávání účtů pomocí předpřipravených filtrů (non-compliant účty, osiřelé účty apod.) | „Doplní dodavatel“ |
| 23 | Funkcionalita | Systém musí podporovat vytvoření hierarchického modelu rolí | „Doplní dodavatel“ |
| 24 | Funkcionalita | Řešení musí obsahovat záchrannou síť proti administrativním manuálním chybám - musí umět simulovat dopad a umožnit náhled před aplikováním změn politik | „Doplní dodavatel“ |
| 25 | Funkcionalita | Řešení umožňuje online synchronizaci dat IDM, zdroje identit a cílových aplikací a nespoléhá pouze na plánované noční batch operace | „Doplní dodavatel“ |
| 26 | Funkcionalita | Systém umí připojit více uživatelských identit k jednomu reálnému uživateli | „Doplní dodavatel“ |
| 27 | Funkcionalita | Systém dokáže spravovat sdílené účty (privilegované uživatele) | „Doplní dodavatel“ |
| 28 | Funkcionalita | Umožňuje monitorovat uživatele používající privilegované účty a umí uchovávat záznamy o historii užívání | „Doplní dodavatel“ |
| 29 | Funkcionalita | Systém dokáže zaznamenat a zpětně přehrát operace, které byly provedeny s pomocí sdílených účtů, a také vyhledávat v tomto záznamu | „Doplní dodavatel“ |
| 30 | Funkcionalita | U privilegovaných účtů uchovává hesla v bezpečném trezoru | „Doplní dodavatel“ |
| 31 | Funkcionalita | Umožňuje měnit hesla sdílených účtů po každém použití pro zachování bezpečnosti | „Doplní dodavatel“ |
| 32 | Funkcionalita | Systém musí být schopen zabezpečit sdílené účty používané aplikacemi a skripty a sledovat jejich aktivity | „Doplní dodavatel“ |
| 33 | Funkcionalita | Systém umožňuje centrální změnu hesla sdíleného účtu bez nutnosti úpravy skriptů a aplikací | „Doplní dodavatel“ |
| 34 | Funkcionalita | Systém umí časově omezit délku využívání sdíleného účtu | „Doplní dodavatel“ |
| 35 | Integrace | Synchronizace hesel a účtů v rámci všech systémů, včetně podpory změny hesla přímo z prostředí Windows desktop | „Doplní dodavatel“ |
| 36 | Integrace | Systém musí podporovat různé operační systémy (Windows Server, Linux, AIX) | „Doplní dodavatel“ |
| 37 | Integrace | Systém musí podporovat různá databázová úložiště (Oracle, MS SQL, IBM DB2) | „Doplní dodavatel“ |
| 38 | Integrace | Systém musí podporovat různé implementace LDAP (MS AD, SAP LDAP, IBM Security Directory Sever, Oracle Directory Server) | „Doplní dodavatel“ |
| 39 | Integrace | Systém musí umožňovat integraci pro správu uživatelů na systémy MS Exchange a Office Online (Office 365) | „Doplní dodavatel“ |
| 40 | Integrace | Komunikace mezi všemi komponentami celého řešení musí probíhat zabezpečeně (např. certifikáty, TLS, SSO) | „Doplní dodavatel“ |
| 41 | Integrace | Systém musí umožňovat podporovat integraci řešení s různými typy autentizace (AD, AD FS, IDM třetích stran, SAML) | „Doplní dodavatel“ |
| 42 | Integrace | Systém obsahuje „out of the box“ základní adaptéry (Unix, Linux, AIX, Active Directory, LDAP, DB2, Oracle DB, Sybase) | „Doplní dodavatel“ |
| 43 | Integrace | Systém v základu obsahuje nástroj pro tvorbu vlastních adaptérů a to v grafickém prostředí a bez nutnosti znalosti programovacích jazyků | „Doplní dodavatel“ |
| 44 | Integrace | Musí nabízet širokou škálu API pro možností přizpůsobení celého systému včetně standardů WebService a REST | „Doplní dodavatel“ |
| 45 | Integrace | Řešení může být nasazeno jako virtual appliance | „Doplní dodavatel“ |
| 46 | Integrace | Řešení musí detekovat změny ve zdrojích identit on-line a následně propagovat do cílových systémů na základě událostí | „Doplní dodavatel“ |
| 47 | Integrace | Systém musí umožňovat organizaci a přemisťování konfiguračních jednotek a balíčků mezi vývojovým, testovacím a produkčním prostředím | „Doplní dodavatel“ |
| 48 | Report | Řešení a jeho reporty musí být akceptovatelné interními i externími auditory, a to v souladu s požadavky ISO 27000 a ZoKB | „Doplní dodavatel“ |
| 49 | Report | Systém umožňuje compliance reporty | „Doplní dodavatel“ |
| 50 | Report | Systém musí umožňovat reportování a následný export reportů do formátů CSV, HTML, PDF a MS Office | „Doplní dodavatel“ |
| 51 | Report | Systém umožňuje report historie změn uživatelů | „Doplní dodavatel“ |
| 52 | UI | Systém bude možné ovládat kompletně z webového rozhraní | „Doplní dodavatel“ |
| 53 | UI | Uživatelské rozhraní podporuje běžné prohlížeče v aktuálních verzích (MS Internet Explorer, Mozilla Firefox a Google Chrome) | „Doplní dodavatel“ |
| 54 | UI | Systém obsahuje Administrátorské rozhraní pro správu aplikace | „Doplní dodavatel“ |
| 55 | UI | Systém obsahuje „Self service“ rozhraní pro koncové uživatele, které musí umožňovat změnu hesla, obnovu zapomenutého hesla, zobrazení seznamu zdrojů a služeb, ke kterým má uživatel přístup, možnost požádat o přístup a také možnost sledovat stav žádostí | „Doplní dodavatel“ |
| 56 | UI | Rozhraní pro administrátory může být upraveno tak, aby zobrazovalo pouze tu část, kterou má administrátor na starosti. | „Doplní dodavatel“ |
| 57 | UI | Základní úkony uživatelů je možné provádět z aplikace pro mobilní zařízení (požadavek na přidělení/změnu přístupu) podporující minimálně platformy Android a iOS. | „Doplní dodavatel“ |
| 58 | UI | Systém musí být plně upravitelný do vzhledu společnosti (web, notifikace, formuláře, reporty, emaily) | „Doplní dodavatel“ |