logo szif

**PŘÍLOHA Č. 10**

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

**Specifikace předmětu plnění**

|  |
| --- |
| **Specifikace předmětu plnění** |

# Vymezení pojmů

Zadavatel pro účely zadávacího řízení vymezuje následující pojmy, které jsou použity v textu Zadávací dokumentace a souvisejících přílohách.

| **Pojem/Zkratka** | **Vysvětlení** |
| --- | --- |
| **Uživatel** | Jedná se o konkrétní fyzickou osobu, kterou lze jednoznačně identifikovat, využívající IS SZIF. |
| **Interní uživatel** | Jedná se o uživatele, který má jakýkoliv pracovně právní vztah k SZIF. |
| **Externí uživatel** | Jedná se o uživatele IS SZIF, který má jiný smluvní vztah k SZIF. |
| **Internetový uživatel** | Jedná se o uživatele, který nemá standardní smluvní vztah k IS SZIF a zároveň využívá IS SZIF (typicky se jedná o žadatele). |
| **Identita** | Znázornění uživatele v nástroji na správu identit. Identifikátor identity konkrétního uživatele je anonymizovaný a je přenášený a využívaný ve všech částech IS SZIF. (Příklad: V prostředí IS SZIF je používán identifikátor pro interní zaměstnance ve tvaru SZIF0NNNN, kdy NNNN vyjadřuje osobní číslo zaměstnance generované v HR systému SZIF). |
| **Role – funkční** | Využíváno pro označení identity s určeným rozsahem oprávnění pro práci v IS SZIF Jedná o souhrn činností a povinností vztahujících se k určité oblasti. |
| **Účet** | Definovaný uživatel s konkrétní identitou v rámci konkrétní aplikace v IS SZIF. (Příklad: konkrétní uživatel s identitou SZIF0NNNN má zřízený účet v konkrétním modulu aplikace SAP CRM s uživatelským jménem a heslem) |
| **Přístupové oprávnění (právo)** | Povolení pro definovaný účet přistupovat ke konkrétnímu objektu pro specifický typ  operace. |
| **Modul** | V prostředí SZIF se primárně jedná o konkrétní aplikační instanci. (Příklad: modul SAP RMP – produktivní instance pro Public Sector Record Management na platformě SAP) |
| **Alerting** | Upozornění správců (uživatelů) systému podle nastaveného pravidla. |
| **SoD – Separation (Segregation) of Duties** | Princip oddělení odpovědností, na základě kterého by neměla mít fyzická osoba více rolí umožňujících provádění několika souvisejících operací ohrožujících informační bezpečnost SZIF. |
| **IS SZIF** | Informační systém SZIF – Významný informační systém dle definice ZoKB, zahrnující primární informační systém na platformě SAP a veškeré další podpůrné i business informační systémy a aplikace, na které se vztahují principy ISMS včetně certifikace ISO 27001, kterou je potvrzeno naplnění podmínek ISMS. |
| **Funkční místo** | Konkrétní přiřazení zaměstnance v rámci organizační jednotky, které definuje činnosti vykonávané konkrétní osobou z hlediska řízení lidských zdrojů. V SZIF je funkční místo definováno např.: ředitel sekce, ředitel odboru, vedoucí oddělení, referent oddělení, referent, asistent, a další. |
| **Organizační jednotka** | Řízená jednotka v rámci organizačního uspořádání fondu sdružující více funkčních míst a osob. V SZIF jsou definovány např. Sekce ICT, Odbor provozu ICT (podřízený Sekci), Oddělení koncových služeb ICT (podřízené Odboru provozu ICT) |
| **ZoKB** | Zákon 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů; ve znění všech prováděcích dokumentů, zejména Vyhlášky 82/2018 Sb. Vyhláška o bezpečnostních opatřeních |
| **ISMS** | Information Security Management System – systém řízení informační bezpečnosti dle definice ISO/IEC 27001:2013 |
| **MD (ManDay)** | Čas odpovídající 8 hodinám práce jedné osoby |

# Obecná specifikace předmětu plnění

Tento dokument stanovuje požadavky na předmět plnění veřejné zakázky. Technická dokumentace, na jejímž základě bude předmět plnění veřejné zakázky realizován, je uvedena v Příloze č. 16 Zadávací dokumentace.

Předmětem plnění bude:

## **Dodávka nástroje IDM nástroje splňujícího požadované technické a funkční vlastnosti**

Dodávka kompletního licenčního vybavení pro zajištění správy:

* 1. 1500 jedinečných produktivně aktivních a uživatelských identit se statusem interní uživatel (zaměstnanec) informačního systému
  2. 250 jedinečných uživatelských identit se statusem externí uživatel
  3. 100000 jedinečných uživatelských identit internetových uživatelů
  4. nástroj musí umět evidovat informace o neaktivních uživatelích – pro interní uživatele je odhadováno celkem 5000 záznamů (aktivní i neaktivní); pro externí uživatele do 800 záznamů (aktivní i neaktivní); pro internetové uživatele až 250000 (aktivní i neaktivní)
  5. počet záznamů musí být možné případně rozšířit parametrově/licenčně
  6. součástí dodávky musí být veškeré licence, nezbytné pro provoz v prostředí zadavatele (tedy např. včetně OS a DB a v rozsahu prostředí dle implementace níže), včetně SW maintenance dodávaných licencí na dobu 60 měsíců ode dne účinnosti smlouvy.

**Kompletní seznam licenčního vybavení uvede Dodavatel v rámci vyplněné Přílohy č. 1 NS:** **Specifikace předmětu plnění.** Dodavatel dále doplní způsob a formát předání oprávněnému zástupci Zadavatele k Akceptaci.

Akceptace této části předmětu plnění bude na základě dodaných licenčních dokumentů a klíčů, instalačních médií, standardní technické specifikace výrobce SW nezbytné pro instalaci IDM nástroje a souvisejícího SW vybavení a následný provoz IDM nástroje a souvisejícího SW vybavení a potvrzení o zajištění maintenance výrobcem nástroje Zadavateli. Veškerá technická dokumentace bude dodána na elektronickém nosiči v digitální podobě.

## **Implementace nástroje**

Implementace bude probíhat formou realizace projektu, který bude řízen v souladu se standardy projektového řízení, nebo agilního projektového řízení. Řízení projektu implementace bude primárně zajišťovat Projekt manager Dodavatele. Koordinaci součinnosti a realizaci na straně Zadavatele (tedy zaměstnanců Zadavatele i ostatních dodavatelů, kteří budou součástí projektu na straně Zadavatele), zajistí Projekt manager Zadavatele.

**Návrh použité metodiky řízení projektu, návrh průběhu a specifikace implementace včetně harmonogramu implementace, požadavků na součinnost a návrhu akceptačních kritérií splňujících parametry ověření funkčnosti dle kapitoly 2.2.4 této Přílohy č. 10 ZD uvede Dodavatel v rámci vyplnění Přílohy č. 1 NS: Specifikace předmětu plnění.**

Maximální doba implementace nástroje v rozsahu specifikovaném níže, je stanovena na nejdéle **80 pracovních dní** ode dne nabytí účinnosti Smlouvy, která bude na základě Zadávacího řízení uzavřena mezi Zadavatelem a Dodavatelem.

Implementace nástroje bude zahrnovat následující oblasti:

### **Instalaci nástroje na virtualizovaném prostředí zadavatele**

1. Instalace nástroje je požadována jako tříúrovňová:
   * + - Vývojové prostředí
       - Testovací prostředí
       - Produktivní prostředí

Nástroj musí být instalován tak, aby byla zajištěna integrita jednotlivých prostředí včetně možnosti organizace a přemisťování konfiguračních jednotek a balíčků mezi vývojovým, testovacím a produkčním prostředí. Nástroj zároveň musí umožňovat v produktivním prostředí IDM porovnávat a spravovat identity a oprávnění v produktivním a testovacím prostředí IS SZIF.

1. Příprava administračního prostředí pro správu IDM nástroje zahrnující minimálně:
   * + - Přípravu systému pro správu organizační struktury
       - Přípravu systému pro správu technických (organizačních) struktur nezávislých na primární organizační struktuře organizace – (pilotní vytvoření projektové organizační struktury a struktury řešitelů dle Servicedesku)
       - Přípravu a definici procesů správy identit
       - Přípravu systému na správu funkčních rolí jednotlivých identit v rámci organizačních (technických) struktur
       - Přípravu a definici procesů správy uživatelů u integrovaných systémů
       - Přípravu a definici schvalovacích workflow pro zajištění správy přístupových oprávnění

### **Plné integraci na:**

1. HR systém Zadavatele – OKBase

Součástí bude příprava automatizovaného rozhraní prostřednictvím webové služby, kdy přenos z HR systému bude standardně zajišťován jednou denně v nočních hodinách. HR systém bude zdrojovým systémem pro zasílání informací o:

* + - * Organizační struktuře Zadavatele – jedná se o organizační strukturu definovanou hierarchickým číslováním (ID) organizačních jednotek a názvem organizačních jednotek.
      * Pracovnících zadavatele – přenášeny budou základní informace o pracovnících zadavatele nezbytné pro další zpracování:

Vytvoření/změnu/zablokování identity,

Začlenění/změnu identity v organizační struktuře,

Určení/změnu funkčních rolí pro vytvořené identity,

Definice/změnu/zablokování uživatelských účtů,

Zřízení/změnu/zablokování přístupových účtů.

HR systém bude **zdrojovým** systémem pro data o pracovnících SZIF, ze kterého bude IDM nástroj data přebírat.

1. Microsoft Active Directory (MS AD) v interním prostředí zadavatele
   * + - Součástí bude integrace na MS AD umožňující

Automatickou správu účtu v MS AD pro zaměstnance zadavatele na základě informace z HR systému Zadavatele

Možnost manuální správy účtu při řešení nestandardních stavů u zaměstnanců zadavatele

Možnost manuální správy účtu externích uživatelských identit definovaných v IDM nástroji

MS AD bude **cílovým** systémem, do kterého bude IDM nástroj informace zasílat.

1. Správu uživatelů (CUA SAP) v informačním systému SAP – v rámci implementace nástroje bude zajištěna kompletní správa uživatelů v CUA SAP a plnou integraci LDAP SAP.

CUA SAP a LDAP SAP bude **cílovým** systémem, do kterého bude IDM nástroj informace zasílat.

U všech definovaných systémů bude možné spustit přenos dat i manuálně pro řešení nestandardních situací.

### **Příprava prostředí pro:**

1. Integraci na jednotlivé dílčí moduly informačního systému SAP - pro umožnění přidělování jednotlivých objektů oprávnění v rámci informačního systému SAP. Předmětem bude návrh postupu a projektového plánu pro zajištění plné integrace na moduly SAP, aby byla v budoucnu zajištěna kromě správy uživatelů v IS SAP i plná administrace objektů oprávnění v informačním systému SAP včetně zákaznicky vyvinutých objektů

Celkový objem prací stanovený pro tuto část nepřekročí 25 MD práce.

1. Integraci na interní podpůrné systémy zajišťující výkon činností SZIF nezbytných pro naplnění ISMS:
   * + - Adonis NP – systém pro správu procesního modelu SZIF
       - ARM – systém řízení rizik
       - Primavera – Systém pro řízení projektů
       - Cognos – webové a BI služby

Předmětem bude návrh postupu pro zajištění integrace na uvedené systémy tak, aby byla zajištěna komplexní integrace IDM nástroje umožňující vytěžování i propagaci dat.

Celkový objem prací stanovený pro tuto část nepřekročí 20 MD práce.

1. Zajištění realizace procesů správy identit a údajů uživatelů IS SZIF prostřednictvím nástroje IDM, tak aby nástroj po provedení do provozu umožňoval standardní správu v následujících oblastech:
   * 1. Řízení business služeb a business procesů – nástroj bude připraven pro definici, správu business procesů, business rolí a budoucí integraci s nástrojem pro správu procesů. Jedná se o Administrátorský proces.
     2. Řízení uživatelských účtů a oprávnění na úrovni Microsoft technologií – kromě integrace s Microsoft Active Directory bude nástroj připraven pro obecnou integraci a správu Microsoft prostředí (typicky Microsoft 365/Azure AD, Exchange). Jedná se o Administrátorský proces.
     3. Řízení uživatelských účtů na úrovni LDAP – příprava nástroje pro řízení uživatelských účtů na úrovni LDAP. Jedná se o Administrátorský proces.
     4. Řízení dalších úrovní uživatelských účtů (internetoví uživatelé) – příprava nástroje pro správu internetových uživatelů, vytvoření definice identit s customizací pro evidenci atributů internetových uživatelů a žadatelů. Jedná se o Administrátorský proces.
     5. Realizace scénářů správy identit (interních, externích, internetových uživatelů)
        + Součástí implementace IDM bude definice scénářů pro správu identit – založení, změna, dočasná změna, vytvoření nového týmu, vytvoření technické organizační struktury, přiřazení identity do technické organizační struktury; příprava základních schvalovacích schémat pro definované scénáře včetně příprava prostředí pro administrátory i ostatní uživatele IDM nástroje. Jedná se o Administrátorský i uživatelský proces
     6. Realizace scénářů pro logování a monitoring včetně monitorování konfliktů oprávnění
        + Součástí implementace IDM bude nastavení základního monitoringu pro logování:
          1. Jakýchkoliv změn na úrovni uživatele/identity/přístupových oprávnění
          2. Systémových operací automaticky realizovaných IDM nástrojem
          3. Operací prováděných administrátory IDM nástroje
          4. Činností prováděných uživateli v IDM nástroji

Jedná se o Administrátorský proces.

* + 1. Řízení správy organizačních struktur včetně definice různých typů organizačních struktur (tvorba technických struktur nezávislých na organizační struktuře organizace dle definovaných parametrů).

Jedná se o Administrátorský proces.

Uživatelské procesy musí být lokalizovány v českém jazyce včetně všech prezentačních vrstev nástroje.

### **Testování funkčnosti IDM nástroje**

V rámci akceptačního testování funkčnosti IDM nástroje bude ověřena integrace na výše uvedené plně integrované systémy s otestováním následujících procesů a distribuce odpovídajících dat na základě realizované integrace:

1. Nástup zaměstnance do pracovního/služebního poměru na dané místo v organizační struktuře:

Zaměstnanec ještě nemá identitu v SZIF – nový zaměstnanec

Zaměstnanec již má identitu v SZIF – návrat zaměstnance na SZIF po přerušeném/ukončeném pracovním/služebním poměru

1. Nástup zaměstnance do pracovního/služebního poměru na neurčené místo v organizační struktuře:
2. Zaměstnanec ještě nemá identitu v SZIF – nový zaměstnanec
3. Zaměstnanec již má identitu v SZIF – návrat zaměstnance na SZIF po přerušeném/ukončeném pracovním/služebním poměru
4. Změna pracovního/služebního poměru zaměstnance
5. Přeřazení zaměstnance na jinou pozici – trvale/dočasně
6. Rozšíření/zúžení přístupových práv zaměstnance na základě změny pracovního/služebního poměru (např. rozšíření po splnění zkoušek státního zaměstnance)
7. Ukončení pracovního/služebního poměru zaměstnance – trvalé/dočasné
8. Změna organizační struktury organizace
9. Přesun organizační jednotky v rámci stávající organizační struktury
10. Vznik/zánik organizační jednotky bez dopadu/s dopadem na stávající zaměstnance
11. Změna náplně v rámci dané organizační jednotky (změna rolí, které mohou zaměstnanci v dané organizační jednotce zastávat)
12. Přečíslování organizačních jednotek v rámci organizační struktury

Dále bude otestována funkčnost nástroje v oblastech:

1. Plná dostupnost a funkčnost prostředí pro administrátory včetně fungování procesů správy uživatelů, identit, rolí, oprávnění, organizačních struktur
2. Plná dostupnost prostředí pro uživatele
3. Plná datová kompatibilita, tj. správnost dat v nástroji na základě ověření aktuálních dat v HR systému, MS AD a CUA SAP
4. Plná funkčnost realizovaných scénářů
5. Plná funkčnost přenosu customizací z vývojového prostředí na produkci.
6. Integrace na jednotlivé systémy a jejich prostředí v rozsahu testovací a produktivní prostředí
7. Plná funkčnost monitoringu prováděných operací

### **Školení administrátorů IDM a zpracování uživatelské a provozní dokumentace**

Veškerá školení (pro administrátorské i uživatelské procesy) budou realizována v českém jazyce. V rámci školení administrátorů a zpracování dokumentace budou požadovány následující činnosti:

1. Proškolení administrátorů IDM, aby bylo možné po uvedení nástroje IDM do produktivního užívaní zajistit:
   * + - Kompletní administrátorské činnosti správy IDM nástroje – instalace, konfigurace, integrace, údržba, patchování, zálohování

Součástí bude proškolení interních administrátorů IDM nástroje zadavatele v rozsahu, který Zadavateli umožní zajistit kompletní administraci a provoz nástroje.

* + - * Implementaci řízení business služeb a business procesů

Součástí bude proškolení interních administrátorů IDM nástroje zadavatele na správu business služeb a procesů v nástroji IDM včetně proškolení na zajištění integrace prostřednictvím webových služeb.

* + - * Řízení uživatelských účtů a oprávnění na úrovni Microsoft technologií – primárně Microsoft Active Directory

Součástí bude proškolení administrátorů IDM nástroje pro správu účtů a oprávnění v MS AD prostřednictvím nástroje IDM.

* + - * Řízení uživatelských účtů na úrovni LDAP

Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na řízení uživatelských účtů na úrovni LDAP.

* + - * Řízení dalších úrovní uživatelských účtů (internetoví uživatelé)

Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na realizaci scénářů správy přístupů internetových uživatelů

* + - * Realizaci scénářů správy identit (interních, externích, internetových uživatelů)

Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele pro zajištění administrace scénářů pro správu identit minimálně v rozsahu připravenosti nástroje.

* + - * Realizaci scénářů pro logování a monitoring včetně monitorování konfliktů oprávnění

Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na správu IDM nástroje v oblasti logování a monitoringu včetně vyhodnocování monitorovaných informací:

1. Jakýchkoliv změn na úrovni uživatele/identity/přístupových oprávnění
2. Systémových operací automaticky realizovaných IDM nástrojem
3. Operací prováděných administrátory IDM nástroje
4. Činností prováděných uživateli v IDM nástroji
   * + - Řízení správy organizačních struktur včetně vícevrstevných organizačních struktur (tvorba technických struktur dle definovaných parametrů)

Součástí bude kompletní proškolení interních administrátorů IDM nástroje zadavatele na ovládání IDM nástroje v oblasti správy organizačních struktur, technických organizačních struktur

1. Tvorba dokumentace, která bude obsahovat následující:
   * + - Kompletní projektová dokumentace k implementaci nástroje v českém jazyce
       - Dokumentace nastavení systému zahrnující protokoly o instalaci, provedení provozních, integračních, bezpečnostních testech, dále dokumentaci o realizovaných customizacích a nastavení IDM nástroje v českém jazyce
       - Administrátorská dokumentace popisující procesy administrátora z hlediska technického nastavení nástroje IDM i z hlediska obsluhy aplikační vrstvy nástroje IDM – pokud bude upravována dokumentace výrobce, může být v anglickém jazyce.
       - Uživatelská dokumentace popisující ovládání nástroje IDM administrátory – pokud bude upravována dokumentace výrobce, může být v anglickém jazyce.
       - Uživatelská dokumentace popisující ovládání nástroje IDM koncovými uživateli – musí být v českém jazyce.

### **Uvedení do produktivního provozu**

Po provedení testování a proškolení administrátorů bude užívání nástroje uvedeno v produktivní provoz a bude akceptována implementace nástroje. V rámci přechodného období 2 kalendářní měsíce produktivního provozu bude zajištěna zvýšená dostupnost podpory dodavatele pro řešení incidentů a problémů.

V rámci produktivního provozu bude dodavatelem zajištěno poskytování aktualizací, patchů a nových verzí nástroje IDM ze strany výrobce zadavateli po celou dobu platnosti SW maintenance (tj. 60 kalendářních měsíců ode dne účinnosti smlouvy) oprávněným osobám (administrátorům nástroje IDM) ze strany Zadavatele. Povinností dodavatele je upozornit zadavatele na každou nově dostupnou aktualizaci, patch, či novou verzi IDM nástroje ze strany výrobce a potvrdit Zadavateli, zda je možné tyto implementovat bez rizika nefunkčnosti jakékoliv produktivně používané části IDM včetně realizovaných customizací.

## **Konzultační a podpůrné služby**

Předmětem plnění bude dále zajištění konzultačních a podpůrných služeb pro další rozvoj IDM nástroje a integraci na ostatní moduly SAP a dotčené informační systémy Zadavatele spočívající v poskytnutí kapacit specialistů (uvedených v seznamu techniků) pro zajištění:

1. Realizace dílčích rozvojových projektů integrace IDM nástroje na nové technologie
2. Zajištění plné integrace nástroje IDM na další části stávajícího IS SZIF

Konzultační a podpůrné služby nejsou paušálně hrazenou činností a jsou alokovány výhradně na základě potvrzené objednávky písemně zaslané (emailem) Oprávněnou osobou Zadavatele a písemného potvrzení schválení Objednávky Oprávněnou osobou Dodavatele. Princip poskytování konzultačních a podpůrných služeb je stanoven v Příloze č. 1 NS: Specifikace předmětu plnění.