Český rozhlas

Vysvětlení zadávací dokumentace č. 2 podle § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon“), k veřejné zakázce č. j. VZ25/2024.

Český rozhlas jako zadavatel tímto poskytuje následující vysvětlení č. 2 k veřejné zakázce č. j. **VZ25/2024** s názvem „**Implementace Identity managementu**“.

Zadavatel dne 21. 1. 2024 obdržel skrze elektronický nástroj JOSEPHINE Žádost o vysvětlení zadávací dokumentace. Zadavatel dává na vědomí, že toto vysvětlení poskytuje v souladu s § 98 zákona ve lhůtě k tomu určené.

Znění dotazu obsahuje celkem 15 otázek, které zadavatel zodpoví postupně. Veškeré dotazy směřují k technické specifikaci (příloha č. 5 Zadávací dokumentace).

Obecně zadavatel dává na vědomí, že technická specifikace obsahuje parametry požadovaného IdM a dodavatelé by měli být schopni zajistit implementaci IdM dle parametrů uvedených v technické specifikaci.

Dotaz č. 1:
„Uvedených 6 měsíců implementace a integrace bere v úvahu nutnou spolupráci s třetími stranami na integraci jejich aplikací?

- *Integrace systémů do IdM obnáší minimálně poskytnutí informací a součinnost třetích stran.*
- *V případech, kdy integrované systémy nemají hotové rozhraní pro vzdálenou správu uživatelů a rolí, je nutné rozhraní vyvinout dodavateli těchto systémů. Zde není možné garantovat dobu nutnou pro realizaci úprav. Při počtu systémů, které je požadováno integrovat, je podle našich zkušeností 6 měsíců příliš krátká doba pro poskytnutí takové součinnosti Zadavatelem.*

Odpověď zadavatele:
Z výsledků předimplementační analýzy by mělo vyplývat, jak bude integrace systémů technicky provedena. Většina systémů, které budou implementovány či integrovány v rámci IdM jsou ve vnitřní síti zadavatele, pod interní správou a jsou napojené na Active Directory. Pro přihlášení do jednotlivých systémů se uživatelé přihlašují za pomoci doménového účtu. Zadavatel nepředpokládá zvýšenou pracnost.

Pro úplnost zadavatel uvádí, že do doby 6 měsíců nebude počítat případné zpoždění, které bude způsobené časem, který potřebují třetí strany na implementaci nového rozhraní pro vzdálenou správu uživatelů a rolí, tj. objektivní okolnosti, kterou zadavatel ani dodavatel nemůže ovlivnit.

Dotaz č. 2:
„Bude vyžadována integrace systémů nativně prostřednictvím specifických konektorů nebo připadá v úvahu (na základě výstupů úvodní analýzy) i integrace mezivrstvou typu DB/CSV?“

Odpověď zadavatele:
Vzhledem k množství proprietárních systémů v prostředí zadavatele je nutné zvažovat i varianty, kdy systémy budou napojené na IdM pomocí mezivrstvy. Identifikace způsobu a technického provedení napojení jednotlivých systémů by mělo být předmětem předimplementační analýzy v rámci Fáze 1.

Dotaz č. 3:

„Integrace všech systémů do IdM bude probíhat v rámci jedné etapy během 6 měsíců?

- *Dle našich zkušeností je optimální napojit základní systémy (obvykle HR a AD), důkladně celé řešení otestovat, zařadit do produkce a teprve následně postupně integrovat další systémy.*
- *Velmi důležitým aspektem implementace IdM je pozitivní přijetí ze strany uživatelů a je tedy nezbytné minimalizovat negativní dopady na jejich fungování.“*

Odpověď zadavatele:
Zadavatel souhlasí s tím, že optimální je začít s napojením základních systémů (HR, AD). U řady systémů je očekáváno napojení přes AD, čímž dojde ke zrychlení nasazení (viz tabulka na poslední straně souboru "Příloha č. 5 – Technická specifikace"). Jak je uvedeno v odpovědi na otázku č. 1., do této doby se nebude započítávat čekací doba na případný vývoj rozhraní třetími stranami.

Dotaz č. 4:
„V Příloze č. 5 je zmíněna studie proveditelnosti, je prosím možné zaslat výstup z této studie?“

Odpověď zadavatele:
Dokument obsahuje interní citlivé údaje, které se zadavatel rozhodl nesdílet. Zároveň zadavatel dává na vědomí, že pro relevantní stanovení nabídkové ceny není tento dokument potřebný. Veškeré potřebné informace zadavatel uvádí v zadávací dokumentaci a jejich přílohách. Zadavatel uvádí, že v rámci úvodní analýzy dostane vybraný dodavatel tento dokument k dispozici.

Dotaz č. 5:
„Jaký je standardní životní cyklus běžného a privilegovaného uživatele?“

Odpověď zadavatele:
V prostředí zadavatele není definované rozdělení běžných a privilegovaných uživatelů. Cyklus běžných a privilegovaných uživatelů v prostředí zadavatele není formálně standardizován a obnáší řadu výjimek. Tento proces bude ukotven v prvotní fázi projektu v rámci detailní analýzy prostředí zadavatele. Na ukotvení procesů bude spolupracovat dodavatel IdM řešení a zadavatel.

Dotaz č. 6:
„IdM umožňuje "vytvořit a přiřadit hierarchickou strukturu oprávnění a skupin".

- *Jsou pro vytvoření této hierarchie (např. pro business role) dostupná strojově čitelná data?*
- *Pokud ne, kolik business rolí je součástí dodávky?“*

Odpověď zadavatele:
Primárním zdrojem dat pro definici business rolí je AD. Dalším zdrojem bude třístupňová hierarchie, která je dostupná v HR modulu SAPu. V rámci prvotní fáze dodávky bude nutné ověřit, že data jsou kompletní a dostačující pro vytvoření samotných business rolí v IdM systému. Pokud data kompletní nebudou, bude nutné chybějící role stanovit v rámci úvodní analýzy, tj. prvotní fáze dodávky ve spolupráci se zadavatelem.

Dotaz č. 7:
„IdM umožňuje "konfiguraci notifikací v libovolném stavu workflow".

- *Kolik typů notifikací (řádově) je součástí dodávky?“*

Odpověď zadavatele:
Zadavatel dává na vědomí, že to momentálně nelze jednoznačně určit. Toto bude v závislosti na tom, kolik workflow bude potřeba vytvořit a jakým způsobem budou jednotlivé aplikace řízeny. V rámci workflow by však relevantní strany měly být informovány o změnách

stavu, výsledku schválení apod. Každá změna stavu ve Workflow by měla umožnit notifikaci, tj. zaslat e-mail o změně stavu.

Dotaz č. 8:
„V bodu "Řízení organizační struktury" IdM umožňuje "kategorizaci uživatelů podle pracovních týmů, projektů nebo specifických rolí".

- *Kolik takových kategorizačních schémat je součástí dodávky?*
- *Jsou pro ně dostupná strojově čitelná data?“*

Odpověď zadavatele:
Tato identifikace bude součástí detailní předimplementační analýzy, a proto zadavatel předem nemůže definovat, kolik kategorizačních schémat je součástí dodávky. Řízení přístupů je řešeno rolemi v rámci Active Directory. Základní organizační struktura Českého rozhlasu je k dispozici v HR modulu SAP.

Dotaz č. 9:
„V bodu "Recertifikační proces” IdM umožňuje “pravidelné revize oprávnění a jejich vynucení".

- *Kolik typů recertifikačních procesů je součástí dodávky?“*

Odpověď zadavatele:
Zadavatel recertifikační procesy definované nemá. Rozdělení typů účtů jednotlivých systémů, jejich identifikace a definice IAM politik bude součástí detailní předimplementační analýzy, které bude tvořena ve spolupráci se zadavatelem.

Dotaz č. 10:
„IdM umožňuje "definovat a vynutit princip segregace povinností (segregation of duties)".

- *Kolik SoD politik je součástí dodávky?“*

Odpověď zadavatele:
Tato identifikace bude součástí detailní předimplementační analýzy. Zadavatel dává na vědomí, že požadavek není možný předem určit. Identifikace toxických oprávnění a řízení systémů bude předmětem konzultace s vlastníky systémů při integraci daného systému.

Dotaz č. 11:
„IdM umožňuje "definici více politik [hesel] tak, aby bylo možné nastavovat různé požadavky pro různé typy účtů".

- *Kolik politik hesel je součástí dodávky?“*

Odpověď zadavatele:
Tato identifikace bude součástí detailní předimplementační analýzy. Bude nutná diskuze ohledně rozdělení typů účtů jednotlivých systémů a definice IAM politik. Zadavatel se domnívá, že nejméně však politika pro běžné uživatele, privilegované uživatele a servisní účty. Nemusí se jednat o konečný výčet.

Dotaz č. 12:
„Napojení systémů:
Jaký je rozsah integrace zdrojových i cílových systémů, které nejsou připojené přes AD? Prosíme o doplnění detailů per-systém:

- *podporované rozhraní*
- *rozsah řízení (CRUD)*
  - *uživatelských účtů, servisních účtů*
  - *skupin, oprávnění*
  - *oprávnění účtů, jejich členství ve skupinách*
  - *organizačních jednotek*
  - *jiných druhů objektů*

Jedná se o tyto systémy:

- *SAP, AIS, ISE + WLAN controller, GSelector, PROVYS, USYS, CDI-VARS, Terminal Server Users, Cisco Meetings Server*

Specificky pro SAP - jaký rozsah integrace SAP Zadavatel očekává?“

Odpověď zadavatele:
Zadavatel dává na vědomí, že detailnější analýza systémů bude součástí předimplementační analýzy.

Integrace, řízení oprávněni, skupin a přístupů systémů se týká primárně systémů, u kterých je v příloze č.1 uvedeno ve sloupci "Napojení na AD", "Přístup skrze AD" a "Oprávnění skrze AD". Řízení mezi budoucím IdM a AD je uvažováno pouze u systémů, u kterých uvedeno ve sloupci "Napojení na AD", "Přístup skrze AD" a "Oprávnění skrze AD". Řízení přístupů u těchto systémů je řešeno přes skupiny a účty v AD.

Zadavatel se pokusil k jednotlivým systémům doplnit detailnější popis:

- *SAP* - Uživatelské a servisní účty je možné napojit z AD, nicméně oprávnění, skupiny apod. jsou řízeny prostřednictvím interních Z* tabulek. Tzn. správa uživatelů a objektů prostřednictvím AD nebo standardním SAP ERP rozhraním a správa oprávnění a skupin pomocí separátního konektoru a úpravu záznamů Z* tabulek.

- *AIS* - Správa prostřednictvím záznamů v Oracle DB. Plné řízení uživatelů, rolí, skupin. Oprávnění na základě členství ve skupinách i samostatně.

- *ISE + WLAN controller* – Nízký počet uživatelů a velmi hrubé řízení oprávnění. Systém není třeba prioritizovat.

- *GSelector* – Rozhraní bude ověřováno s dodavatelem. V aplikaci je třeba řídit správu uživatelů, rolí a oprávněních.

- *PROVYS* – Nastavení, správa rolí a oprávnění v současné době provádí dodavatel (3. strana).

- *USYS* - Systém je možné integrovat pomocí AD. Nyní však dochází k manuálnímu vytváření uživatelů, rolí a přiřazování oprávnění.

- *CDI-VARS* - Pro aplikaci je nutné zajistit provizi uživatelů a přiřazování rolí (lze AD skupinou).

- *Terminal Server Users* - Aplikace umožňuje napojení přes AD.

- *Cisco Meetings Server* - Dostupné API rozhraní, detaily nutné ověřit s dodavatelem. Provize uživatelů a přiřazení AD skupiny.

V případě SAP počítá zadavatel s integrací na IdM pouze v oblasti přebírání organizační struktury zadavatele a uživatelský entit (například HPP, DPP/DPČ, externista).

Dotaz č. 13:
„Softwarové prostředí:

- *Naše dodávka sestává z aplikačního serveru a databáze.*
- *Do jakého stavu přípravy prostředí vstupuje se svou dodávkou Dodavatel a co spravuje na SW úrovni?*
  - *Čistý HW a kompletní instalace Dodavatelem?*
  - *Čistý operační systém?*
  - *Balíčky a další?*

- *Jakou formu dodávky Zadavatel očekává? Jak probíhá nasazování nových verzí dodávky?*
    - *Git repository, docker image, CI-CD konfiguraci a další?*
- *Kdo instaluje a spravuje databázi IDM (PostgreSQL)?*
- *IdM umožňuje "zálohování dat do separátních databází" a také obnovu ze zálohy na úrovni databáze. Je implementace zálohování a obnovy DB součástí dodávky?*
- *Kdo spravuje testovací prostředí? Kdo spravuje produkční prostředí?*
    - *Vytvoření, nasazování a další?“*

Odpověď zadavatele:
Zadavatel má svou vlastní infrastrukturu a virtualizační platformy. HW a operační systém je ve správě zadavatele.

Dodavatel by měl být na základě parametrů v technické specifikaci dodat kompletní dodávku. Forma i způsob, jakým probíhá nasazování nových verzí je na uvážení dodavatele.

Databázi IdM instaluje dodavatel. Implementace zálohování není součástí dodávky. Úkolem dodavatele je stanovit co/kdy/jak je zapotřebí zálohovat a jakým způsobem je možné zálohu obnovit.

Dotaz č. 14:
„HA a škálování:

- *IdM má "umožnit zajištění vysoké dostupnosti"*
    - *(pozn. IdM není kritickou komponentou infrastruktury, v případě výpadku nedojde k narušení funkčnosti prostředí uživatelů. HA tedy není standardně v projektech IdM vyžadována.)*
    - *Požaduje Zadavatel v dodávce HA konfiguraci, nebo jen její podporu ze strany produktu?*
    - *HA je vyžadováno na úrovni aplikačního serveru, nebo i na úrovni databáze?*
- *IdM má "umožnit hladké zvýšení výkonu"*
    - *pozn. s ohledem na počet identit v prostředí Zadavatele nepředpokládáme na základě našich zkušeností potřebu výrazného navyšování výkonu prostředí IdM).*
    - *Požaduje Zadavatel v dodávce konfiguraci automatického škálování, nebo jen její podporu?*
    - *Jaké rozhraní prostředí Zadavatel případně poskytuje?*

Odpověď zadavatele:
Zadavatel se domnívá, že systém IdM je kritickou součástí infrastruktury, neboť zajišťuje efektivní a bezpečnou správu identit a přístupů.

Zadavatel dává na vědomí, že HA konfiguraci primárně nepožaduje (není uvedena v technické specifikaci). Podporu obecně požaduje v režimu SLA, jak je uvedeno v technické specifikaci.

Zadavatel primárně nepožaduje v dodávce konfiguraci automatického škálování, pouze obecnou podporu v režimu SLA.

Dotaz č. 15:
„Prvotní školení běžných uživatelů:

- *Je součástí dodávky proškolení všech běžných uživatelů Dodavatelem nebo část uživatelů, a pokud ano, tak kolik?*
- *Je možné školení běžných uživatelů vyřešit nahrávkou školení?“*

Odpověď zadavatele:
Zadavatel nepožaduje školení všech uživatelů, ale jak je v tabulce pro výpočet ceny uvedeno, ale zaškolení administrátorů a klíčových uživatelů. Přesný počet není zadavatel

schopen v tuto chvíli stanovit. Zadavatel odhaduje školení pro 20 - 30 uživatelů, přičemž výčet nemusí být konečný. Pro uživatele je možné vytvořit uživatelské příručky a video manuály formou nahrávky.

Na základě tohoto vysvětlení zadávací dokumentace č. 2 zadavatel prodlužuje lhůtu pro podání nabídek o 3 celé pracovní dny.

Digitálně podepsal
Mgr. Petra
Barášková
24.01.2025 20:24

Mgr. Petra Barášková
Oddělení veřejných zakázek
Český rozhlas