SPRÁVA ŽELEZNIC

Naše zn. 47909/2025-SŽ-GŘ-O25

Věc: Vysvětlení zadávací dokumentace č. 1

Sektorová nadlimitní veřejná zakázka dle § 56 zákona č. 134/2016 sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „Zákon") na služby s názvem:

„**Nasazení systému IdM v prostředí Správy železnic**"

Správa železnic, státní organizace (dále jen „Zadavatel") obdržela dne 26. 6. 2025 v 08:39 hodin žádost o vysvětlení zadávací dokumentace. Zadavatel formou Vysvětlení zadávací dokumentace odpovídá na tuto žádost doručenou k veřejné zakázce následovně:

Dotaz č. 1:

Bod 20.15.3. Zvláštních obchodních podmínek pro Zakázky v oblasti ICT uvádí, že Provozovatel je povinen *„provádět pravidelné zálohy dat a programového vybavení vztahujících se k Plnění dle Smlouvy, zabezpečit je vhodnými prostředky proti neoprávněným přístupům nebo jejich ztrátě a v pravidelných intervalech testovat funkčnost těchto záloh, nejméně jedenkrát za měsíc, není-li ve Smlouvě ujednáno jinak*."
Chápeme správně, že toto zálohování, zabezpečení proti neoprávněným přístupům a testování funkčnosti, provádí Provozovatel s využitím Služeb zálohování Zadavatele popsaných v příloze ZD „Platforma SŽ Standardy zálohování a disaster recovery", tj. Provozovatel nezálohuje žádnou část řešení na vlastních zálohovacích technologiích?

Odpověď č. 1:

Ano, Zadavatel potvrzuje, že zálohování zajistí Zadavatel stávajícím technickým řešením popsaným v Příloze č. 9 Zadávací dokumentace – Platformě SŽ.

Dotaz č. 2:
Může zadavatel potvrdit, že poptává jednu IdM sondu (2 node) pro jednu technologickou síť?

Odpověď č. 2:

Zadavatel poptává jednu IdM sondu (2 node geograficky oddělené) pro soubor technologických sítí. Tato sonda bude obsahovat pouze identity, které mají přiřazenou nějakou roli v některé z technologických sítí (více v kapitole 4.2.6 Přílohy č. 2 zadávací dokumentace - Bližší specifikace předmětu plnění veřejné zakázky (Technická specifikace)).

Dotaz č. 3:
Může Zadavatel potvrdit, že požaduje mít v režimu HA i repozitář s daty IdM řešení?

Odpověď č. 3:

Zadavatel k uvedenému dotazu sděluje, že celé řešení musí být v režimu HA v souladu s Bližší specifikací předmětu plnění veřejné zakázky (Technická specifikace) článek 4.2.1 Instalace IdM

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném
Městským soudem v Praze, spisová značka
A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

("*Produkční instance bude provozována v režimu HA*") a 4.2.6 Systémové a licenční požadavky.

Dotaz č. 4:

Může Zadavatel upřesnit, zda pro účely HA režimu je možné využít stávající LoadBalancer Zadavatele?

Odpověď č. 4:

Ano, v prostředí UAS (uživatelské sítě) lze využít stávající load balancer Zadavatele (více v kapitole 6.2 Přílohy č. 9 zadávací dokumentace - Platforma SŽ verze 2.2). V prostředí technologických datových síti technologie typu load balancer není k dispozici.

Dotaz č. 5:

Může zadavatel upřesnit, zda všichni uživatelé autentizující se do IdM budou ověřováni proti jediné instanci Active Directory?

Odpověď č. 5:

V souvislosti s uvedeným dotazem se Zadavatel odkazuje na Přílohu č. 2 zadávací dokumentace - Bližší specifikace předmětu plnění veřejné zakázky (Technická specifikace), konkrétně na článek 4 Požadavky na plnění ("*Dodávka a implementace nástroje IdM a jeho integrace se zdrojovými systémy, vícero instancemi (foresty) AD, JIRA a zapojenými systémy (30 zapojených systémů)*").

Zadavatel v této souvislosti sděluje, že řešení předpokládá napojení koncových aplikací prostřednictvím vícero instancí MS AD. V UAS existují aktuálně trustované foresty v řádu jednotek. V rámci technologické sítě bude vytvořeno několik nezávislých forestů MS AD v řádu vyšších jednotek (dle aktuálního stavu, který v budoucnu může být změněn).

Autentizace do IdM bude vůči vícero instancí (domén) MS AD.

Dotaz č. 6:

Může zadavatel upřesnit, jaké informace budou při obousměrné integraci poskytovány z Active Directory do IdM?

Odpověď č. 6:

Při oboustranné integraci budou poskytovány veškeré informace nutné pro zajištění ověření správnosti předávaných dat, případně všechny atributy, které AD schéma umožňuje evidovat/předávat. Teoreticky se může jednat o libovolný atribut.

Dotaz č. 7:

Předpokládá Dodavatel správně, že IdM bude při zakládání emailových schránek komunikovat výhradně s onprem instancí Exchange?

Odpověď č. 7:

Ano IDM prvotně vytvoří schránku v on-prem prostředí, ale musí si poradit i se situací, kdy je schránka migrována do cloudu, aby nevytvářel znovu schránku v on-prem prostředí. Zadavatel využívá hybridní prostředí Exchange v rámci jedné Exchange organizace. Bližší informace o požadavcích na životní cyklus identit je uveden v Příloze č. 2 zadávací dokumentace - Bližší specifikace předmětu plnění veřejné zakázky (Technická specifikace) článek 4.2.1.1 Požadavky na životní cyklus identit. Bližší informace o požadavcích na životní cyklus identit jsou uvedeny v

kapitole 4.2.1.1 Přílohy č. 2 zadávací dokumentace - Bližší specifikace předmětu plnění veřejné zakázky (Technická specifikace),

Dotaz č. 8:

Předpokládá Dodavatel správně, že některá požadovaná workflow budou pouze součástí IdM sondy?

Odpověď č. 8:

Ano, tento scénář je vysoce pravděpodobný a bude záviset na navrhovaném řešení.

Dotaz č. 9:

V kap. 2.1 ZD „Očekávání od implementace řešení" v odstavci „Požadavky na rozsah řešení" v bodě č. 4 Zadavatel uvádí:
„Zprovoznění a otestování integrací systémů dodavatelů třetích stran integrovaných skrze AD"
Může Zadavatel upřesnit požadovaný rozsah prací Dodavatele na "Zprovoznění a otestování integrací systémů dodavatelů třetích stran integrovaných skrze AD"?

Odpověď č. 9:

Jedná se o činnosti nutné k provedení testu všech usecase typických pro IdM z pohledu propagace do koncového systému. Zadavatel rozumí, že napojení koncového systému do AD nemůže Dodavatel IdM ovlivnit, nicméně se primárně jedná o spolupráci při onboardingu aplikací, poskytnutí součinnosti při testování a optimalizaci rozhraní napojovaných systémů.

Dotaz č. 10:

V kap. 4.2.1.1 ZD „Požadavky na životní cyklus identit" v bodě č. 17 Zadavatel uvádí: "*Přístup externích správců oprávněných osob, kteří budou pouze ve vlastní organizační skupině (vlastní organizační struktuře) spravovat své identity a žádat o jejich role. Nová žádost o identity zadaná externím správcem do IdM je prostřednictvím integrace odesílána do SAP formou žádosti a následně v SAP po přidělení ID a validaci zařazena do odpovídající organizační struktury a odeslána zpět do IdM s ostatními identitami a aktivována.*" Může Zadavatel potvrdit, že zdrojem dat pro „externí správce oprávněných osob" a "vlastní organizační struktury externistů" je SAP HR?

Odpověď č. 10:

Zadavatel uvádí, že primárním zdrojem dat pro všechny uživatele (včetně externích identit) je SAP HR, žádost o vytvoření identity může vzniknout i v jiném systému, než je SAP (např. IDM, JIRA, atd.).

Dotaz č. 11:

V kap. 3 ZD „Současný stav a popis prostředí" v odstavci „Koncové (cílové) systémy" v bodě č. 4 Zadavatel uvádí:
"*systémy typu Privileged Access Management (PAM) pro správu technických, servisních a správcovských účtů*"
Může Zadavatel potvrdit, že aplikace PAM je napojená na Active Directory podobně jako jiné aplikace a není tedy přímo řízena z IdM?

Odpověď č. 11:

Ano, PAM je napojen na AD, ale členství v AD bude řízeno IDM.

Dotaz č. 12:

V kap. 4.2.1.1 ZD „Požadavky na životní cyklus identit" v bodě č. 16 (Dodávku následujících reportů) Zadavatel uvádí: "*Report účtů, ke kterým existuje v IdM vlastník, ale které vznikly mimo vědomí IdM*." Může Zadavatel upřesnit požadavek, resp. podmínku, kdy "v IdM existuje vlastník, ale vznikl mimo vědomí IdM"?

Odpověď č. 12:

Všichni současní vlastníci vznikli mimo vědomí IdM, jelikož IdM nebylo doposud využíváno a nasazení nástroje IdM do prostředí Zadavatele je součástí této veřejné zakázky. Popisovaný stav v otázce bude nastávat např. v budoucnu u všech nově onboardovaných aplikací/systémů do IdM. V této souvislosti se dále Zadavatel odkazuje na bod 4.8 Přílohy č. 2 zadávací dokumentace – Bližší specifikace předmětu plnění veřejné zakázky (Technická specifikace), který blíže popisuje předmět Služeb na vyžádání tak, že tyto zahrnují:

- *"Poskytnutí až 500 MD, které bude moci Zadavatel využít k v rámci zvýšené technické podpory, k rozvoji nástroje IdM nebo vytvoření přímé integrační vazby s dalšími systémy provozovanými SŽ (zdrojové/koncové systémy)*
- *integraci dalších koncových systémů do nástroje IdM pomocí AD´s".*

Závěr

Zadavatel zcela setrval na zadávacích podmínkách. Lhůta pro podání nabídek se tak nemění a je stanovena na 11. 7. 2025, 10:00 hod.

Ing. David Miklas
01.07.2025 11:11
Podepsáno
elektronicky

……

Ing. David Miklas
Ředitel organizační jednotky
Správa železniční telematiky