



Zadavatel:

Dopravní podnik Ostrava a.s.

se sídlem: Poděbradova 494/2, Moravská Ostrava, 702 00 Ostrava

IČO: 61974757

Veřejná zakázka:

„IdM – Identity Management“

sektorová veřejná zakázka na dodávky zadávaná v režimu zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“)

Vysvětlení zadávací dokumentace

dle ust. § 98 a § 99 ZZVZ

Zadavatel, Dopravní podnik Ostrava a.s., obdržel ve výše nadepsaném zadávacím řízení žádost dodavatele o vysvětlení zadávací dokumentace. V návaznosti na obdrženou žádost zadavatel uvádí znění dotazu a připojuje příslušné vysvětlení.

Žádost o vysvětlení zadávací dokumentace č. 1 (obdržena dne 15. 12. 2017):

Zadavatel v příloze č. 1 ZD — Technická specifikace požaduje, aby IdM obsahovalo autentizační server, který bude umožňovat zprostředkovat systémům autentizační úlohy přes následující protokoly/standarty:

- LDAP (ActiveDirectory)
- Windows autentizaci
- Rádus
- Ověření pomocí certifikátu
- Podpora vícefaktorové autentizace

Dotaz č. 1:

Znamená to tedy, že Zadavatel požaduje, aby nově dodávaný IdM systém nejen distribuoval identitní informace (uživatelské účty, skupiny, role, apod.) ale uchovával i hesla pro autentizaci distribuovaných identit?

Dotaz č. 2:

Pokud ano, počítá Zadavatel s tím, že IdM systém nahradí stávající autentizační server MS Active Directory?



Dotaz č. 3:

V případě, že Zadavatel požaduje zachování stávajícího autentizačního serveru MS Active Directory, který umí všechny výše uvedené protokoly, lze pro zajištění požadavku na autentizační server využít funkcionalitu MS Active Directory a provést pouze jeho integraci?

Informace zadavatele k žádosti č. 1 (poskytnuty dne 20. 12. 2017):

Ad 1)

Zadavatel nepožaduje, aby IdM systém uchovával hesla pro autentizaci distribuovaných identit.

Ad 2)

Zadavatel nepožaduje náhradu za stávající autentizační servery MS Active Directory.

Ad 3)

Zadavatel požaduje zachování stávajících autentizačních serverů MS Active Directory a jejich integraci s IDM systémem.

Žádost o vysvětlení zadávací dokumentace č. 2 (obdržena dne 27. 12. 2017):

Dotaz č. 1:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 4 uveden požadavek: "Zadavatel požaduje licencování formou multilicence".

Rozumíme správně tomu tak, že licenční model požadovaného systému IdM nesmí být omezen na počet uživatelů a tím pádem musí umožnit správu licenčně neomezeného počtu uživatelů?

Dotaz č. 2:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 7 uveden požadavek: "V IdM bude správce moci konfigurovat pravidla pro automatické začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě atributů identity a přidružených referenčních objektů. (organizační jednotka, aplikační role, systematizované místo atd.)."

Rozumíme správně tomu tak, že pravidla mají být aplikovatelná na nějaký atribut uživatele a nějaký referenční objekt nebo jakýkoliv libovolný? Je požadováno, aby pravidla kombinovala více hodnot a referenčních objektů v jednom pravidle současně?

Dotaz č. 3:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 10 uveden požadavek: "IdM bude obsahovat workflow pro řízení životního cyklu změn identit."

Prosíme o konkretizaci, co všechno musí tato workflow splňovat za požadavky.



Dotaz č. 4:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 12 uveden požadavek: "IdM bude obsahovat minimálně logy, které zaznamenávají události systému, změnu entit evidovaných v systému, změny konfigurace nastavení systému IdM, průběh synchronizací IdM s dalšími systémy."

Je požadováno, aby tyto logy byly součástí portálu IdM? Je požadováno, aby byly logy k dispozici pouze v textovém souboru nebo mají být zapracovány do formulářů a seznamů přímo v uživatelském rozhraní portálu IdM?

Dotaz č. 5:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 26 uveden požadavek: "Portál IdM bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do Portálu IdM a následně tato oprávnění přiřazovat konkrétním uživatelům."

Prosíme o upřesnění a rozvedení detailních požadavků na editor rolí a na co mají být práva nastavena.

Dotaz č. 6:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 24 uveden požadavek: " IdM umožní notifikovat emailovou zprávou vytvoření a změny identity."

Žádáme o uvedení popisu detailních požadavků na požadované notifikace. Z požadavku není jasné, jak mají notifikace vypadat a na jaké události přesně reagovat.

Dotaz č. 7:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 36 uveden požadavek: "Splnění požadavků GDPR."

Žádáme o upřesnění požadavku. Z popisu není jasné, jestli IdM má obsahovat evidenci osobních údajů.

Dotaz č. 8:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" jsou v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM v bodě 12 a 22 uvedeny požadavky: " IdM bude obsahovat minimálně logy, které zaznamenávají události systému, změnu entit evidovaných v systému, změny konfigurace nastavení systému IdM, průběh synchronizací IdM s dalšími systémy.

Veškeré požadavky změn, 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 a konfiguraci IdM. Záznam v historii bude obsahovat původní i novou hodnotu."

Rozumíme správně tomu tak, že změny, které budou prováděny v portálu IdM, budou v IdM logovány a je požadováno prohlížení logů a jejich vyhledávání přímo v portálu IdM? Jaké jsou požadavky na zpřístupnění těchto logů?



Dotaz č. 9:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM uveden požadavek: " Systém bude integrován s aplikacemi třetích stran".

Jaké režimy synchronizace jsou požadovány v systému IdM pro napojení na uvedené systémy v zadávací dokumentaci? Je možné využít synchronizace, která bude reagovat pouze na změny a nebude pracovat se všemi záznamy v systému?

Dotaz č. 10:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" jsou uvedeny požadavky pro akceptaci řešení systému IdM.

Rozumíme tomu správně tak, že i v rámci nabídkového řízení bude zadavatel požadovat předvedení splnění vybraných požadavků na systém IDM z přílohy č. 4?

Dotaz č. 11:

V zadávací dokumentaci veřejné zakázky "IdM - Identity Management" je v dokumentu Příloha č. 4 ZD – Požadavky na funkcionality IdM uveden požadavek: " Systém bude integrován s aplikacemi třetích stran".

Požaduje zadavatel zahrnout do nabídkové ceny řešení IdM rovněž případné finanční náklady na straně systémů třetích stran, na které se má systém IdM dle požadavků zadávací dokumentace integrovat?

Informace zadavatele k žádosti č. 2 (poskytnuty dne 2. 1. 2018):

Ad 1)

Zadavatel požaduje, aby systém nebyl licenčně omezen počtem uživatelů.

Ad 2)

Zadavatel požaduje, aby pravidla mohla být aplikovatelná na libovolný atribut a musí umožňovat kombinaci více hodnot a více podmínek současně.

Ad 3)

Zadavatel specifikuje blíže požadavky na workflow následovně:

- Zadání požadavku uživatelem na nová nebo změněná oprávnění ke schválení;
- Zadání požadavku uživatelem na změnu v přiřazení rolí a skupin ke schválení;
- Sledování stavu svého požadavku uživatelem;
- E-mailové upozornění schvalovatele na čekající požadavek na schválení;
- Seznam úloh (přehled činností) pro každého schvalovatele;
- Schválení/zamítnutí požadavku;
- Podpora vícekrokového schvalování;
- Podpora schvalování jedním nebo více schvalovateli (i skupinou schvalovatelů);
- Možnost větvení WF pro ošetření výjimek při schvalování;
- Řešení zastupitelnosti;



- Eskalace – nedodržení termínu, neschválené požadavky schvalovatelem (na nadřízeného, případně na další osobu);
- Možnost vložení systémových kroků s voláním webových služeb a spuštění skriptů;
- Sledování průběhu WF v grafickém vyjádření – diagram o stavu WF. Diagram v obvyklém formátu pro WF – aktivita diagram, BPMN, Archimate apod.

Ad 4)

Zadavatel požaduje zpracování logů ve formulářích portálu IdM.

Ad 5)

Zadavatel požaduje, aby oprávnění pro přidělení uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části IS (identity, referenční objekty, notifikace, synchronizace, konfigurace systému, reporty, WF, webové služby apod.)

U jednotlivých částí bude možnost definování akce pro činnosti uživatele v konkrétní části IDM s daným oprávněním. Pro identity a referenční objekty bude možnost definice oprávnění k jejich atributům s možností zobrazení/nezobrazení atributu, editace atributu uživatelem, povinnost nastavení/vyplnění atributu, pořadí zobrazení atributu.

Na úrovni organizační jednotky bude možno pro výběr a přiřazení role nastavit sady povolených aplikačních rolí, skupin a systematizovaných míst dostupné pro identity z dané organizační jednotky.

Ad 6)

Zadavatel požaduje zajištění zasílání konfigurovatelných emailových upozornění systému minimálně, pro tyto události:

- Vytvoření identity a referenčního objektu
- Změny identity a referenčního objektu (systemizované místo, organizace, jednotka, skupina, agenda, aplikace, aplikační role, skupina aplikací atd.)
- Problém při synchronizaci, při vypršení hesla v AD
- Vypršení platnosti certifikátu

Zasílání těchto upozornění bude možno v předstihu. Velikost předstihu (ve dnech) musí být konfigurovatelná pro jednotlivé typy upozornění. K dispozici budou šablony upozornění, kde bude možno definovat příjemce, předmět, obsah upozornění. Bude umožněno do šablony vložit libovolný atribut identity a/nebo referenčního objektu. Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext/podmínky za jakých bude odesláno. V konfiguraci bude možno využít atributů identit a referenčních objektů.

Ad 7)

Zadavatel požaduje, aby systém IDM obsahoval evidenci subjektů osobních údajů, kategorie, klasifikace osobních údajů a účel správy osobních údajů.

Ad 8)

Zadavatel požaduje, aby veškeré požadavky na změny bylo možné zadávat pouze přes portál IdM. Není přípustné zadávat požadavky na změny prostřednictvím ruční změny v textových souborech, případně xml, CSV apod. z důvodu zajištění logování všech změn u jednotlivých konfigurovatelných parametrů IdM.



IdM bude obsahovat export přehledů a seznamů zobrazených na portále do souborů CSV, případně jiného strojově zpracovatelného a současně běžně čitelného formátu. Veškeré změny vyvolané požadavkem uživatelem nebo správcem v IdM budou probíhat transakčně. Budou logovány tak, aby bylo možno kdykoliv dohledat a prokázat provedené změny v identitách, referenčních objektech, atributech, v konfiguraci a v administraci IdM. Záznam logu bude obsahovat původní i novou hodnotu. IdM umožní export auditního reportu z údajů o identitách uložených v IdM a to i historických. Auditní report bude min. obsahovat souhrnné zobrazení daných uživatelů (identit) jejich rolí v IS napojených na IdM, rolí, přiřazených skupin v aktuálním okamžiku i do minulosti. Výstup auditního logu bude ve strojově zpracovatelném a současně běžně čitelném formátu příkladně XML, CSV. Identity pro generování auditního reportu musí být možné vybírat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.

Ad 9)

Zadavatel uvádí, že pro napojení a implementaci synchronizace IdM s jednotlivými IS bude umožněno více režimů synchronizace:

- Plná synchronizace – projde všechny objekty IdM a synchronizuje se systémem
- Změnová synchronizace – synchronizace změn od poslední události synchronizace, včetně uchování informace o události, kterou synchronizace vyvolala.
- Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.
- Simulační synchronizace – vytvoření reportu očekávaných změn v napojeném systému po provedení ostré synchronizace.

Ad 10)

Zadavatel nebude požadovat v rámci nabídkového řízení předvedení splnění vybraných požadavků na systém IdM z přílohy č. 4 zadávací dokumentace – Požadavky na funkcionality IdM.

Dodavatel je povinen výše uvedenou přílohu vyplnit dle pokynů, které zadavatel uvedl v bodu 3.4.1. zadávací dokumentace.

Ad 11)

Zadavatel požaduje, aby cena zahrnovala veškeré náklady nezbytné k řádné realizaci předmětu plnění, včetně nákladu na dopravu do plnění, nákladů na provedení zkušebního provozu předmětu. V ceně díla budou již zahrnuty všechny autorské a recyklační poplatky, tak jak je uvedeno v Závazném návrhu smlouvy o dílo, článku V – Cena díla, bodu 5.2., který tvoří přílohu č. 2 zadávací dokumentace.

V Ostravě dne 02. 01. 2018

Dopravní podnik Ostrava a.s.

Poděbradova 494/2

702 00 Ostrava, Moravská Ostrava
18

Bc. Karla Holušová

úsek ředitele nákupu a služeb