Ostravská univerzita
Dvořákova 7 / 701 03 Ostrava / Česká republika
telefon: +420 597 091 002
web: osu.cz

IČ: 61988987 / DIČ: CZ61988987
ID datové schránky: 37gj9fm
Bankovní spojení: ČNB Ostrava, č.ú: 931761/0710

Vyřizuje: Konečná/sara.konecna@osu.cz

Všem dodavatelům

Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE

1.1. Název veřejné zakázky:	**„Dodávka softwaru IDM včetně implementace na OU“**
1.2. Identifikační údaje o zadavateli	
Název:	Ostravská univerzita
Sídlo:	Dvořákova 7, 701 03 Ostrava
IČ:	61988987
1.3. Veřejná zakázka podle předmětu:	Veřejná zakázka na dodávky
1.4. Druh zadávacího řízení:	Zjednodušené podlimitní řízení

Na základě žádosti účastníka o vysvětlení zadávací dokumentace podle § 54 odst. 5 a § 98 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „zákon“) poskytuje zadavatel následující vysvětlení.

Dotaz č. 1:
V ZD v příloze 1 - Technická specifikace je uveden požadavek:
"IDM musí poskytovat strojové rozhraní (WSDL, REST, SOAP), které umožní správu objektů evidovaných v rámci IDM"

Prosíme o detailní výčet metod nebo objektů, které mají být obsaženy v požadovaném rozhraní. Případně jak má být rozhraní zabezpečeno, nastaveno logování provozu atd.

Odpověď č. 1:
Zadavatel k tomuto dotazu uvádí, že IDM musí podporovat alespoň jedno rozhraní REST nebo SOAP, kde budeme mít možnost/metody pro načtení osoby nebo kolekci osob k pracovišti a jejich oprávnění. Přesnější specifikace bude provedena v rámci implementační analýzy. Zabezpečení předpokládáme přes token, logování provozu alespoň na úrovni klient a volané metody.

Dotaz č. 2:
V ZD v příloze 1 - Technická specifikace je uveden požadavek:
"Administrátorské rozhraní musí umožnit správu objektů evidovaných v IDM."

Rozumíme správně, že se jedná o objekty osob, identit, uživatelských účtů, organizační struktury, skupin, pracovních pozic, rolí, oprávnění pro přístup do administrátorského rozhraní IDM, "notifikačních šablon", reportů, konektorů a synchronizačních úloh, pravidel pro automatizaci, workflow, žádostí, konfigurace systému atd.?

Odpověď č. 2:
Zadavatel k tomuto dotazu uvádí, že v administrátorském rozhraní požadujeme minimálně správu objektů osob, identit, uživatelských účtů, organizační struktury, skupin, pracovních pozic, rolí, oprávnění pro přístup do administrátorského rozhraní IDM a synchronizačních úloh. Vše ostatní zmíněné musí být pro administrátora IDM konfigurovatelné jiným jednoduše dostupným způsobem.

Dotaz č. 3:
V ZD v příloze 1 - Technická specifikace je uveden požadavek:
"Administrátorské rozhraní musí mít možnost nastavit práva jednotlivým privilegovaným uživatelům (správcům), aby bylo možno nastavit správce s nižším oprávněním (např. read-only)."

Rozumíme správně, že v rámci administrátorského rozhraní má být možné definovat libovolné oprávnění do obrazovek, atributů, sloupců v seznamech a akcí, které je možné v administrátorském rozhraní vykonávat? A že následně je požadováno toto oprávnění přiřazovat jednotlivým uživatelským rolím jako například správce organizační jednotky, vedoucí pracovník, správce konektoru, správce konfigurace IDM, skupin, globální správce, auditor atd.? Nebo tomu máme rozumět tak, že bude v systému jenom jedna role správce? Případně pak ještě read-only správce?

Odpověď č. 3:
Zadavatel k tomuto dotazu uvádí, že předpokládáme, že budou vytvořena dvě rozhraní: administrátorské a uživatelské.
Administrátorské rozhraní bude určeno pouze administrátorům systému IDM. V něm potřebujeme mít minimálně role administrátora IDM (práva na vše) a read-only přístup pro vybrané osoby.
Pro uživatele (či vedoucí pracovníky) předpokládáme přístup do uživatelského rozhraní, kde budou k dispozici pouze formuláře (workflow) na konkrétní procesy.

Dotaz č. 4:
V ZD v příloze 1 - Technická specifikace je uveden požadavek:
"Aplikační rolí se rozumí role pro konkrétní aplikaci, někdy je označována jako technická role nebo přímo oprávnění (např. table-xyz-read)"

A dále pak
"IDM musí podporovat parametrizované přiřazení role uživateli nebo skupině, kde mezi minimální množinu parametrů patří – datum počátku platnosti přiřazení, datum konce platnosti přiřazení."

Prosíme o upřesnění, jestli je v IDM požadováno pro role spravovat a umožnovat přidělené role včetně i nějakého parametru jako například zmíněné oprávnění, kódy organizačních jednotek, platnosti atd. Případně prosíme o vysvětlení, jak bylo myšleno.

Odpověď č. 4:
Zadavatel k tomuto dotazu uvádí, že požadujeme, aby IDM evidovalo aplikační role, a bylo schopné je přiřadit uživateli či skupině (v připojených cílových systémech). Přiřazení role k uživateli či skupině bude možno buď na základě schvalovacího procesu (workflow), nebo automaticky na základě daných parametrů (například příslušnost k organizační jednotce, datum platnosti přiřazení apod.).

Dotaz č. 5:
V ZD v příloze 1 - Technická specifikace je uveden požadavek:
"IDM musí umožnit konfigurovat další reporty (a emailové upozornění) na základě definovaných událostí nebo změn."

Rozumíme tomu správně tak, že administrátorské rozhraní IDM má obsahovat editor pro vytváření libovolných reportů a libovolných emailových upozornění na základě událostí a dat, která jsou v systému IDM obsažena? Nepředpokládáme, že do těchto reportů a emailových notifikací mají být zahrnuta data a události, která v systému IDM nejsou k dispozici.

Odpověď č. 5:
Zadavatel k tomuto dotazu uvádí, že nepožadujeme, aby konfigurace reportů a notifikací byla přímo součást administrátorského rozhraní, pokud bude možno je konfigurovat jiným jednoduše dostupným způsobem. Tyto reporty a notifikace budou vytvářeny pouze na základě dat a událostí, které jsou IDM k dispozici.

Dotaz č. 6:
Prosíme o potvrzení, že zajištění „OpenLDAP temporary“, proxy overlay, a migrace dat z „Novell eDirectory“ je zajištěn na straně objednavatele. IDM bude následně zajišťovat správu „OpenLDAP temporary“ dle požadavků.

Odpověď č. 6:
Zadavatel k tomuto dotazu uvádí, že nikoliv. Požadujeme, ať dodavatel zajistí instalaci a konfiguraci OpenLDAP (jak „hlavní“ instance, tak temporary instance včetně zprovoznění proxy overaly). Export dat z Novell eDirectory zajistí objednatel, import těchto dat do OpenLDAP temporary zajistí dodavatel. IDM bude následně zajišťovat správu objektů i v OpenLDAP temporary.

Dotaz č. 7:
V rámci etapy 1 jsou uvedeny následující požadavky:
- IDM bude evidovat právě jednu identitu pro každého studenta, navázaná studia budou evidována odděleně
- IDM bude v systému OpenLDAP temporary (náhrada za Novell eDirectory) řídit účty pro tyto typy identit:
o student (studium) – účty reprezentující jednotlivá studia studenta, účty již existují

Chápeme správně, že v rámci IDM systému je zavedena jedna identita studenta (obsahující atributy jako jméno, příjmení, osobní číslo apod.), která má pro „OpenLDAP temporary“ evidováno více účtů (pro jednotlivá studia studenta)? Bude existovat v „OpenLDAP temporary“ atribut pro seskupení účtů studenta k identitě (identifikátor osoby, osobní číslo apod.)?

Odpověď č. 7:
Zadavatel k tomuto dotazu uvádí, že v současné době může pro jednoho studenta existovat více účtů (pro každé jeho studium jeden). Atribut pro seskupení účtu k identitě existuje – kmenové číslo. V IDM bude pro každého studenta evidována jen jedna identita. V OpenLDAP temporary bude pro ni dočasně vytvořeno více účtů (pro každé studium jedno). Tento dočasný stav bude sloužit pro zachování zpětné kompatibility se současným modelem identit. V rámci fáze 2 budou tyto účty v OpenLDAP temporary zrušeny.

Dotaz č. 8:
IDM bude spravovat více adresářových služeb (AD, OpenLDAP, OpenLDAP temporary). Jsou nebo nejsou v systémech shodné loginy pro účty jedné identity? Případně uveďte pro jednotlivé typy identit, pokud se to liší (zaměstnanec, externista, …).

Odpověď č. 8:
Zadavatel k tomuto dotazu uvádí, že v současných systémech (AD a Novell eDirectory) se loginy mohou lišit. OpenLDAP temporary prozatím neexistuje. Loginy se mohou lišit i po importu dat do OpenLDAP temporary. Jedním z cílů nasazení IDM je i sjednocení loginů. Tedy ve finálním stavu (po fázi 2) by měly být loginy stejné.

Dotaz č. 9:
V zadávací dokumentaci nejsou zmíněna další prostředí. Předpokládá se tedy vytvoření pouze produkčního IDM prostředí, které bude napojeno na odpovídající produkční zdrojové i cílové systémy?

Prosíme o upřesnění, zda bude požadováno vytvořit a udržovat i nějaké testovací prostředí. Při takto složitém projektu bychom to očekávali.

Odpověď č. 9:
Zadavatel k tomuto dotazu uvádí, že OU nemá prostředky na vytvoření kompletní testovacího prostředí se všemi systémy, které budou napojené na IDM, ale budeme požadovat po dodavateli, aby vytvořil ve spolupráci se zadavatelem částečné testovací prostředí (např. testovací IDM server a k tomu některé testovací kopie napojených systému).

Tímto vysvětlením zadávací dokumentace nebyla provedena změna zadávacích podmínek.

V Ostravě dne ……

Bc. Sára Konečná
Digitálně podepsal Bc. Sára Konečná
Datum: 2022.11.03 09:36:14 +01'00'

……
Bc. Sára Konečná
referent oddělení veřejných zakázek