MINISTERSTVO ZEMĚDĚLSTVÍ

MZE-40484/2025-12121

mzedms029479210

SP. ZN.: MZE-40484/2025-12121
Č. J.: MZE-40484/2025-12121

VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 6

Název veřejné zakázky:	Dodávka, provoz a rozvoj Identity management systému
Druh zadávacího řízení:	Užší řízení dle § 58 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“)
Zadavatel:	Česká republika – Ministerstvo zemědělství
Sídlem:	Těšnov 65/17, 110 00 Praha 1 – Nové Město
Zastoupený:	Ing. Vladimírem Velasem, zastupujícím ředitelem Odboru informačních a komunikačních technologií
IČO:	00020478

Česká republika – Ministerstvo zemědělství jako zadavatel výše uvedené veřejné zakázky obdržel dne 14.05.2025 žádost o vysvětlení zadávací dokumentace. Níže uvádíme její úplné znění společně s odpovědí zadavatele.

Dotaz č. 1:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „5.2 Fáze 2 – Návrh architektury a design klíčových částí IDM“ se hovoří:

„Ukončení této fáze a další pokračování v projektu je podmíněno úspěšným akceptováním Návrhu architektury a designu klíčových částí IDM, které konstatuje, že Řešení neobsahuje vady kategorie A.“

Předpokládáme správně, že slovo „vady“ by mělo být nahrazeno slovem „nedostatky“?

Odpověď zadavatele na dotaz č. 1:

V rámci předání výstupů jednotlivých fází jsou ve smlouvě použity dva pojmy „vada“ a „nedostatek“, Zadavatel považuje oba pojmy v rámci Smlouvy, v kontextu předání výstupů plnění Poskytovatele, za synonyma.

Dotaz č. 2:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „5.2 Fáze 2 – Návrh architektury a design klíčových částí IDM“, může Zadavatel blíže specifikovat nebo více rozvést „Nedostatek kategorie A“? Zároveň prosíme o informaci, jakým způsobem by navržené řešení mohlo porušovat „best practice“ v oblasti ICT, zejména pak v oblasti kybernetické bezpečnosti.

Odpověď zadavatele na dotaz č. 2:

Zadavatel je přesvědčen, že v případě „Nedostatků kategorie A“ je zřejmé, co bude obsahem posouzení pro klasifikace nedostatku do této třídy, tj. 1) pokrytí všech funkčních a nefunkčních požadavků uvedených ve Smlouvě a za 2) návrh a realizace provedena takovým způsobem, aby nedošlo k porušení obecně akceptovaných „best practice“ zásad v oblasti ICT a kybernetické bezpečnosti. V případě „best practice“ se jedná o nedodržení požadavků a doporučení vyplývajících z běžně akceptovaných dokumentů např. ISO 27000, doporučení NÚKIB, požadavků Národního architektonického plánu; v případě poskytování ICT služeb je to použití metodiky ITIL v4; obecně soulad s právními předpisy v oblasti eGovernmentu České republiky a právními předpisy ošetřujícími oblast kybernetické bezpečnosti; a dále například neošetření známých zranitelností na jakékoliv úrovni v rámci připravovaného řešení. Některé další konkrétnější požadavky na vývoj, dokumentaci, tvorbu architektonických modelů, tvorbu hesel, šifrování, správu informačních aktiv atd., jsou součástí dokumentů předávaných Uchazeči oproti podpisu NDA.

Dotaz č. 3:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „3.1 Požadavky na architekturu Řešení“, Zadavatel v části "Autentizace a autorizace IDM" požaduje napojení IdM na SSO:

"*Všechny součásti Řešení musí být napojeny na jednotný autentizační a autorizační systém Objednatele a implementovat SSO.*“

Z uvedeného vyplývá, že uživatelé IdM budou autentizováni proti SSO třetí strany a tedy nesmí/nemohou mít uložené autentizační údaje uživatelů.

V další části "Řízení hesel" v kapitole „3.2.5 Požadavky na bezpečnost“, Zadavatel požaduje řídit hesla, kde uvádí, že "*Politiky hesel bude možné přiřazovat jednotlivým řízeným systémům nebo samotnému IDM systému, takže budou při změně hesel z IDM rozhraní aktivně vynucovány. Pro hesla do IDM systému bude možné vynucovat také neopakovatelnost stejného hesla za posledních N změn (historie hesel).*"

Z uvedeného vyplývá, že IdM musí mít uložené autentizační údaje IdM uživatelů včetně historie hesel.

V této souvislosti máme dva dotazy:

Co je myšleno jednotným autentizačním a autorizačním systémem Zadavatele?

Pokud jde o existující systém, jehož implementace není předmětem této VZ, tak je druhý požadavek (kapitola 3.2.5) podle našeho názoru v rozporu s požadavkem prvním (kapitolou 3.1): pokud se IdM autentizuje proti externímu IdP, neukládá autorizační údaje, ale druhý požadavek předpokládá, že IdM s autorizačními údaji pracuje. Může Zadavatel upřesnit výše uvedené požadavky?

Odpověď zadavatele na dotaz č. 3:

„Jednotný autentizační a autorizační systém Zadavatele“, nebo také „systém autorizace a autentizace MZe“ je systém, který vystupuje v roli IdP a implementuje protokol OIDC pro účely autentizace a autorizace.

Jak zmíněno v odstavci 3.3.3.5:

> *„Přihlášení pomocí **OIDC** prostřednictvím definovaného IdP. Zmíněný IdP nemusí být implementován před nasazením příslušné funkcionality IDM, ale IDM musí OIDC podporovat, aby bylo možné po nasazení jednoduše doimplementovat.“*

Z tohoto důvodu je nutné, aby IDM podporoval jak možnost přihlášení pomocí jména a hesla, tak i prostřednictvím externí autentizace/autorizace využívající protokol OIDC. V požadavcích nevidíme rozpor, neboť:

- Mezi metodami přihlášení by mělo být možné konfiguračně přepínat, jak uvedeno v požadavku požadavku P-32.
- Systém může sloužit k uchovávání autentizačních údajů (například pro účely provisioningu do cílových systémů), přičemž zároveň umožňuje uživatelům přístup do systému IDM prostřednictvím externí autentizace přes IdP.

Dotaz č. 4:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „3.3 Specifické požadavky na funkcionalitu a vlastnosti Řešení“, je v požadavku P-28 uvedeno: „*Přihlášení bude chráněno řešením, které zamezí zamčení účtů uživatele při brute force attacku.*“

Rozumíme správně, že Zadavatel požaduje implementovat tuto ochranu Dodavatelem? Domníváme se, že v případě, že bude autentizace uživatelů do IdM probíhat přes SSO Access Manageru Zadavatele (*jednotný autentizační a autorizační systém viz. výše*), není možné zajistit ochranu proti brute force attacku na straně systému IdM implementovaného v rámci této veřejné zakázky. Může Zadavatel požadavek upřesnit, případně upravit?

Odpověď zadavatele na dotaz č. 4:

Jak zmíněno v odstavci 3.3.3.5:

„Přihlášení uživatele do IDM systému bude možné jedním z následujících způsobů:

- *Přihlášení prostřednictvím **lokálního IDM hesla a loginu přiřazeného k IDM Profilu** spolu s **druhým faktorem autentizace**, který je momentálně předmětem rozvoje na straně objednatele, tudíž jeho integrace bude předmětem analýzy.*

- *Přihlášení pomocí **OIDC** prostřednictvím definovaného IdP. Zmíněný IdP nemusí být implementován před nasazením příslušné funkcionality IDM, ale IDM musí OIDC podporovat, aby bylo možné po nasazení jednoduše doimplementovat.“*

Zmíněný požadavek P-28 se tedy vztahuje k prvnímu způsobu autentizace, kdy se uživatel přihlašuje pomocí jména a hesla. Pro běžné uživatele bude k ochraně proti útokům typu brute force využit druhý faktor (MFA) objednatele. Technické a administrátorské účty mohou být chráněny dostatečným hardeningem, přičemž pro externí přístupy admistrátorů bude využit systém PIM.

Dotaz č. 5:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „3.3 Specifické požadavky na funkcionalitu a vlastnosti Řešení“, je v požadavku P-32 uvedeno: „*Přihlášení uživatele do IDM systému je možné jedním z následujících způsobů: Přihlášení prostřednictvím uživatelského jména a lokálního IDM hesla a dalším faktorem. Přihlášení pomocí OIDC požadavku na systém autorizace a autentizace MZe. Mezi výše zmíněnými metodami je možné konfiguračně přepínat.*“

Může Zadavatel upřesnit, zda je myšleno přepínání způsobu autentizace na úrovni identity / profilu nebo na úrovni rozhraní (Administrátorské / Interní / Externí), případně jinak?

Odpověď zadavatele na dotaz č. 5:

Konfigurace způsobu přihlašování musí být možná na úrovni jednotlivých rozhraní (Administrátorské / Interní / Externí).

Dotaz č. 6:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, v kapitole „3.3.2.4 Import organizační struktury“ Zadavatel uvádí databázi CODEL.

Bude Zadavatel při návrhu integrace schopen poskytnout technickou dokumentaci k API (JDBC, REST, SOAP, ...) této databáze?

Odpověď zadavatele na dotaz č. 6:

Zadavatel předá dokumentaci ke CODEL DB vybranému uchazeči VZ pro potřeby návrhu integrace s IDM. Aktuálně informujeme, že k DB CODEL je možné připojení pouze přes Oracle NET - tedy připojení standardní databázovým connect stringem.

Dotaz č. 7:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „4. Požadavky na provoz systému“, v požadavku P-54 Zadavatel specifikuje použití databáze Oracle 19c nebo MS SQL Enterprise 2014. V požadavku „P-55“ je uvedena možnost využít pro provoz IdM kontejnerizaci OpenShift.

Dovolujeme si Zadavatele upozornit na skutečnost, že některá řešení pro IdM mohou být optimalizována pro konkrétní databáze z pohledu dostupných funkcí a výkonnosti systému a také může být podpora systému ze strany vendora vázána na konkrétní (novější) typy používaných databází. Pokud Zadavatel omezí možnost použití databáze na Oracle nebo MS SQL a to navíc relativně staré verze, může tím velmi omezit možnost výběru konkrétního produktu pro tuto veřejnou zakázku.

V této souvislosti pokládáme dotaz, zda je možné použití jiné databáze (např. PostgreSQL) nebo novější verze Oracle nebo MSSQL za předpokladu, že Dodavatel zajistí licenční podporu, provoz, zálohování a monitoring bez jakéhokoli nároku na provozní podporu ze strany Zadavatele?

Pokud by se Dodavatel rozhodl využít kontejnerizaci OpenShift dle „P-55“, je možné využít Crunchy PostgreSQL, které je možné použít v rámci technologie OpenShift, za předpokladů uvedených v předchozím odstavci?

Odpověď zadavatele na dotaz č. 7:

Zadavatel připouští použití pouze databází Oracle 19C a všech vyšších verzí a databáze MS SQL Enterprise 2014 a všech vyšších verzí.

Dotaz č. 8:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, v kapitole „3.3.2.9 Katalog aplikací“ Zadavatel uvádí katalog aplikací CMBD (iTOP).

Bude Zadavatel při návrhu integrace schopen poskytnout technickou dokumentaci k API (JDBC, REST, SOAP, ...) tohoto katalogu?

Odpověď zadavatele na dotaz č. 8:

Zadavatel poskytne vybranému dodavateli požadovanou technickou dokumentaci k API. V případě iTOP se jedná o API REST JSON.

Dotaz č. 9:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, v kapitole „3.3.1.5 Notifikace“ je požadováno zasílat notifikace o blížícím se konci platnosti hesla koncového účtu.

Chápeme správně, že jde o požadavek na zasílání notifikace o konci platnosti hesla, které si uživatel v koncovém systému změnil prostřednictvím samoobsluhy v IdM? V jiných případech nemá IdM o konci platnosti hesla informaci a nemůže proto posílat notifikace.

Odpověď zadavatele na dotaz č. 9:

Ano. Je tím myšleno zasílání notifikací o blížícím se konci platnosti hesla koncového účtu, které bylo změněno prostřednictvím IDM. Je brána v potaz pouze informace o poslední změně hesla iniciované ze systému IDM.

Dotaz č. 10:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „3.3 Specifické požadavky na funkcionalitu a vlastnosti Řešení“, požadavek „P-32“ uvádí Zadavatel, že: *Přihlášení uživatele do IDM systému je možné jedním z následujících způsobů:*

- *„Přihlášení prostřednictvím uživatelského jména a lokálního IDM hesla a dalším faktorem.“*

Obvykle funkcionalitu MFA (další faktor autentizace) zajišťuje Access Management, nikoliv Identity Management, který je předmětem dodávky v rámci této veřejné zakázky. Je pro MFA možné využít existujícího Access Managementu Zadavatele (*jednotný autentizační a autorizační systém* – viz. Dotaz č. 3)?

Odpověď zadavatele na dotaz č. 10:

Jak zmíněno v odstavci 3.3.3.5:

„Přihlášení uživatele do IDM systému bude možné jedním z následujících způsobů:

- *Přihlášení prostřednictvím **lokálního IDM hesla a loginu přiřazeného k IDM Profilu** spolu s **druhým faktorem autentizace**, který je momentálně předmětem rozvoje na straně objednatele, tudíž jeho integrace bude předmětem analýzy.*

- *Přihlášení pomocí **OIDC** prostřednictvím definovaného IdP. Zmíněný IdP nemusí být implementován před nasazením příslušné funkcionality IDM, ale IDM musí OIDC podporovat, aby bylo možné po nasazení jednoduše doimplementovat.“*

Zmíněný požadavek P-32 se tedy vztahuje k prvnímu způsobu autentizace, kdy se uživatel přihlašuje pomocí jména, hesla a MFA objednatele.

Dotaz č. 11:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „3.3.2.2 Import uživatelů“, Zadavatel uvádí, že pro import uživatelů SZIF je zdroj LDIF soubor.

Jedná se o plný export do LDIF formátu nebo o rozdílový export uživatelů?

Odpověď zadavatele na dotaz č. 11:

Jedná se o plný export.

Dotaz č. 12:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „3.3.2.6 Žádost o správu profilu nebo identity“, Zadavatel v žádosti o správu profilu nebo identity uvádí, že: *„Pro akci vytvoření a modifikaci je schvalovateli před schválením umožněno ještě změnit hodnoty atributů profilu/identity.*“

Může Zadavatel uvést, jaký je konkrétní případ užití?

Dovolujeme si Zadavatele upozornit, že z pohledu odpovědnosti za vstupní data není vhodné, aby někdo jiný, kdo v procesu má schvalovat, prováděl modifikaci vstupních dat bez vstupu nebo kontroly osoby, která žádost do procesu zadala. To je proti smyslu kontroly 4 očí - jeden vytvoří/modifikuje, druhý schvaluje.

Je tento požadavek možné vyřešit tak, že žádost bude zamítnuta s výzvou k úpravě vstupních dat, včetně doplnění detailů a zadání nové žádosti?

Odpověď zadavatele na dotaz č. 12:

Zmíněný požadavek má případ užití například v případě zjevného překlepu nebo doplnění chybějících údajů. Tento typ žádosti je vhodné vnímat spíše jako přípravu vstupních dat pro zodpovědnou osobu (schvalovatele), než jako plnohodnotný schvalovací proces. Návrh řešení uvedený v dotazu není uvažován.

Dotaz č. 13:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, „Příloha č. 1 Specifikace IDM a poskytovaných Služeb“, kapitola „3.3.2.10.1 Agregace požadavků a notifikací“, Zadavatel uvádí, že: *„V případě zamítnutí bude schvalovatel požádán o vyplnění důvodu pouze jednou, poznámka bude poté kopírována do jednotlivých požadavků.*“

Může Zadavatel uvést jaký je praktický případ užití, ve kterém je možné důvod zamítnutí hromadně doplnit duplicitně ke všem požadavkům v té samé agregaci? Jedná se přeci o jednu hromadnou agregaci požadavků a IdM bude evidovat jednu poznámku ke všem těmto agregovaným požadavkům.

Odpověď zadavatele na dotaz č. 13:

Schvalovateli je umožněno vybrat nesourodou množinu jednotlivých požadavků, které zamítne s jedním společným odůvodněním (poznámkou). Tyto požadavky mohou být různého typu a pocházet z různých časových období. „Kopírování" odůvodnění do každého požadavku zvlášť je pouze jednou z možností technické implementace. Variantou, kterou považujeme za akceptovatelnou, je také evidence jednoho odůvodnění provázaného se všemi vybranými požadavky.

Dotaz č. 14:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy", „Příloha č. 2 Specifikace Služeb", kapitola „3. KATALOGOVÉ LISTY", „Paušální služby", „ID: IDM-004" je uvedena následující „Požadovaná úroveň Služeb":

- *„Produkční prostředí: BRONZ."*
- *„Testovací prostředí: BRONZ."*
- *„Preprodukční prostředí: TEST."*

Vzhledem k tomu, že u všech ostatních Katalogových listů jsou požadované úrovně služeb:

- *„Produkční prostředí: BRONZ."*
- *„Testovací prostředí: TEST."*
- *„Preprodukční prostředí: TEST",*

prosíme Zadavatele o potvrzení, zda nejde v tomto případě o chybu a nemá být uvedena stejná Požadovaná úroveň jako u ostatních Katalogových listů.

Odpověď zadavatele na dotaz č. 14:

Zadavatel informuje, že se nejedná o chybu. Úrovně služeb jsou v dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy" nastaveny v souladu s požadavky Zadavatele.

Dotaz č. 15:

V dokumentu s názvem „Požadavky na dokumentaci", kapitola „6.1 Formální požadavky" uvádí Zadavatel:

- *„Jedná-li se o významný informační systém, je zdokumentováno, jakým způsobem jsou naplněny požadavky zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákon č. 104/2017 Sb., a některé další zákony."*

Pokud bude implementovaný systém zařazen do kategorie kritické infrastruktury, je pravda, že povinnosti spojené s určením, oznámením NÚKIB a dalšími náležitostmi bude zajišťovat Zadavatel?

Odpověď zadavatele na dotaz č. 15:

Systém není a nebude zařazen do kategorie kritické infrastruktury. Systém není ani dle současné legislativy určen jako významný informační systém ani jako kritická informační infrastruktura.

Dotaz č. 16:

V dokumentu s názvem „Požadavky na dokumentaci“, kapitola „6.1 Formální požadavky“ uvádí Zadavatel:

- „*Naplnění požadavků zákona č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony pokud je to pro systém relevantní.*“

Je v rámci této zakázky nutné zohlednit také novou směrnici NIS2, která je součástí zákona o kybernetické bezpečnosti?

Odpověď zadavatele na dotaz č. 16:

Zadavatel prohlašuje, že každý systém Zadavatele musí naplňovat aktuální legislativu dle znění konkrétního zákona. Aktuální znění připravovaného zákona dle NIS2 ještě není platné. Zadavatel nepředpokládá v novém zákoně výrazné změny v oblasti „technické“ bezpečnosti. V případě, že by přesto došlo k nutným změnám, které by požadoval nový zákon, a tyto nebyly součástí předmětu VZ, využije Zadavatel k takové úpravě rozvojový katalogový list a takovou změnu si u vybraného dodavatele objedná.

Dotaz č. 17:

V dokumentu s názvem „Příloha č. 1 ZD – Závazný text návrhu smlouvy“, kapitola „12.2“ Zadavatel uvádí požadavek „*Veškeré prvky Monitoringu musí být nasazeny na infrastruktuře Objednatele*“.

Dovolujeme si Zadavatele upozornit, že v zájmu efektivity a úspory nákladů je běžnou praxí, že dodavatelé provozují centrální monitorovací řešení, které přijímá monitorovací informace ze sond, umístěných v infrastruktuře zákazníka (komunikace je vždy iniciována jen zevnitř infrastruktury zákazníka). V této souvislosti žádáme Zadavatele o zvážení a případnou úpravu tohoto požadavku tak, aby bylo uvedené řešení monitoringu možné a tím umožnil nabídnout nižší cenu implementačního projektu i následné podpory v porovnání s variantou, kdy Dodavatel bude budovat nový monitorovací systém v infrastruktuře Zadavatele.

Odpověď zadavatele na dotaz č. 17:

Zadavatel disponuje v současné době monitorovacím nástrojem Zabbix a Sitescope. Pro naplnění požadavků smlouvy bude zadavatel požadovat po dodavateli specifikace transakcí a dohledové scénáře. Výstupy z monitoringu budou dodavateli zpřístupněny. V případě, že dodavatel bude trvat na použití jiného monitorovacího nástroje, pak celý monitoring musí být vybudován na infrastruktuře zadavatele.

Vzhledem k tomu, že zadavatel neuveřejnil vysvětlení zadávací dokumentace do 3 pracovních dnů, prodlužuje lhůtu pro podání nabídek v souladu s § 98 odst. 4 ZZVZ, tedy o jeden pracovní den. Nabídky je tedy možné podat **do 28.05.2025, 11.00 hodin.**

V Praze dne: *shodné s datem a časem el. podpisu*

Ing. Vladimír Velas
Digitální podpis: 20.05.2025 15:44

Česká republika – Ministerstvo zemědělství
Ing. Vladimír Velas
zastupující ředitel odboru informačních a komunikačních technologií