Zadavatel:
Dopravní podnik Ostrava a.s.
se sídlem: Poděbradova 494/2, Moravská Ostrava, 702 00 Ostrava
IČO: 61974757

Veřejná zakázka:
„IdM – Identity Management II.“

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 26. 04. 2018):

Dotaz č. 1:
Požadovaná architektura? Dvě nebo tři vrstvy?

Dotaz č. 2:
Tři vrstvy – databázová, aplikační a prezentační

Dotaz č. 3:
Dvě vrstvy – databázová a aplikační

Dotaz č. 4:
Na jaké platformě by měl běžet portál? Java? .NET C#? PHP?

Dotaz č. 5:
Upřednostnění nějaké platformy?

Dotaz č. 6:
Je požadován tlustý klient nebo je stěžejní pouze Portál?

Dotaz č. 7:
Předpokládá se možnost správy na úrovni L2 a nižší vlastními silami (databáze)?

Dotaz č. 8:
Zdroje? Kde jsou umístěny (doména? DMZ? Cloud?), jaká podporují rozhraní (SQL view? Webservice?), jaká je dostupnost (online? dávky?), existuje licenční omezení (individuální účty? Technický účet?)

- Personální data (Helios?)
- Organizační struktura (Helios?)
- Pracovní místa (Helios?)
- Aplikace
- Aplikační Role
- Uživatelské role
- Alvao – Dokumentace k ServiceDesku?
- DMS – Konkrétně jaký?
- Korund – Co to je? Je k dispozici dokumentace?
- BIS – Docházkový systém Je k dispozici dokumentace?
- Gist controlling – Co to je? Je k dispozici dokumentace?
- Sprinter – Dispečerský systém pro dopravní podniky - Je k dispozici dokumentace?
- MYQ – Co to je? Je k dispozici dokumentace?
- Syslog a a SIEM – Je k dispozici dokumentace?

Dotaz č. 9:
Mobilní zařízení Android a iOS (pouze response design webu? Nebo nativní aplikace?)

Dotaz č. 10:
Šifrování dat – požadované algoritmy a standardy mimo jiné v souvislosti s GDPR?

Dotaz č. 11:
Rozsah šifrování?

Dotaz č. 12:
Navazující aplikace seznam a popis?

Dotaz č. 13:
Konektory popis?

Dotaz č. 14:
Požadované funkce – popis funkcí?

Dotaz č. 15:
Korund, Gist, Sprinter, MYQ – popis konektorů, požadovanou funkčnost API?

Dotaz č. 16:
Má webová aplikace být schopná instalace na uvedených OS, nebo pouze využívaná?

Dotaz č. 17:
Práce s databázemi – správa – její obsah? – propojení s aplikacemi?

Dotaz č. 18:
Vícefaktorová autentifikace?

Dotaz č. 19:
Osoba musí být certifikovaná výrobcem. Jak se postupuje v případě, že se jedná o vlastní produkt?

Informace zadavatele k žádosti č. 1 (poskytnuty dne 02. 05. 2018):

Ad 1)
Zadavatel tento požadavek úmyslně nespecifikoval z důvodu oslovení co největšího počtu potencionálních dodavatelů.

Ad 2)
Zadavatel neporozuměl vznesenému dotazu, avšak uvádí, že popis uvedený dodavatelem odpovídá třívrstvé architektuře.

Ad 3)
Zadavatel neporozuměl vznesenému dotazu, avšak uvádí, že popis uvedený dodavatelem odpovídá dvouvrstvé architektuře.

Ad 4)
Zadavatel požadavek na platformu portálu úmyslně nespecifikoval. Požadavky na funkčnost portálu však specifikoval v příloze č. 1 ZD – Technická specifikace - Požadavky na Portál IDM.

Ad 5)
Zadavatel neupřednostňuje žádnou platformu z důvodu oslovení co největšího počtu potencionálních dodavatelů.

Ad 6)
Tlustý klient není zadavatelem požadován.

Ad 7)
Zadavatel předpokládá možnost spravování na úrovni uživatele. Správu databáze zadavatel požaduje v rozsahu standardních činností.

Ad 8)
Zadavatel specifikoval požadavky na zdroje, jejich umístění a rozhraní v příloze č. 1 ZD – Technická specifikace - Základní požadavky.

- Personální data (Helios?)
  - ANO
- Organizační struktura (Helios?)
  - Ano
- Pracovní místa (Helios?)
  - Ano
- Aplikace
  - Rejstřík aplikací bude obsahovat nástroj IDM – uvedeno v Příloze č. 1 ZD. Dále se předpokládá činnost s privilegovanými účty v aplikacích, které uvedl v příloze č. 1 ZD – Technické specifikace.

V nástroji je Správa aplikací založená na zabezpečení systému, aplikace a uživatelského profilu, který obsahuje: přístupové role, věk, riziko, nepopiratelnost vykonaných činností.
Nástroj umožňuje správu účtu pro systémové služby či systémové aplikace.

- Aplikační Role
  - obsahuje nástroj IDM
- Uživatelské role
  - obsahuje nástroj IDM
- Alvao – Dokumentace k ServiceDesku?
  - Dokumentace je k dispozici na: https://www.alvao.cz/
- DMS – Konkrétně jaký?
  - Zadavatel nemůže zveřejnit tyto informace, z důvodů stále probíhajícího výběrového řízení k tomuto systému.
- Korund – Co to je? Je k dispozici dokumentace?
  - Dokumentace je k dispozici na: http://www.tescosw.cz/planovani-a-rizeni-udrzby/korund/joby/
- BIS – Docházkový systém Je k dispozici dokumentace?
  - Dokumentace je k dispozici na: http://www.eskon.cz/cz/
- Gist controlling – Co to je? Je k dispozici dokumentace?
  - Dokumentace je k dispozici na: http://www.gist.cz/cz/produkty/business-intelligence
- Sprinter – Dispečerský systém pro dopravní podniky - Je k dispozici dokumentace?
  - Dokumentace je k dispozici na: http://www.herman.cz/cs/produkty/isrd/dispecerske-systemy/sysdp/
- MYQ – Co to je? Je k dispozici dokumentace?
  - MYQ označuje řešení pro správu tisku. Dokumentace je k dispozici na: https://www.myq-solution.com/cs/, produkt „Business Pro“
- Syslog a SIEM – Je k dispozici dokumentace?
  - Nástroj není nasazen

Ad 9)
Zadavatel tento požadavek úmyslně nespecifikoval z důvodu oslovení co největšího počtu potencionálních dodavatelů.

Ad 10)
Zadavatel nechává použití algoritmů na možnostech dodavatelů, v souvislosti s GDPR, viz. příloha č.1 ZD – Technická specifikace, GDPR.

Ad 11)
Zadavatel specifikoval požadavky na šifrování v příloze č. 1 ZD – Technická specifikace v části: dodávka HW (switch) - Šifrování/zabezpečení 802.1x RADIUS,SSH

Ad 12)
Zadavatel uvedl seznam a popis aplikací v příloze č. 1 ZD - Technická specifikace v části: Požadavky na webové služby IDM v oblasti požadovaných konektorů a integrace na stávající aplikace.

Ad 13)
Zadavatel uvedl popis konektorů v příloze č. 1 ZD – Technická specifikace v části: Požadavky na webové služby IDM v oblasti požadovaných konektorů.

Ad 14)
Zadavatel uvedl požadavky a popis funkcí v příloze č. 1 ZD – Technická specifikace v části: Základní požadavky a Požadavky na portál IDM.

Ad 15)
Zadavatel požaduje propojení nástroje IDM s uvedenými informačními systémy. Jejich popis je uveden v příloze č. 1 ZD – Technická specifikace. Dodavatel je povinen zajistit plnou integraci s uvedenými systémy na vlastní náklady s přednostním využitím API u jednotlivých informačních systémů.

Ad 16)
Zadavatel nechává řešení webové aplikace na dodavateli.

Ad 17)
Zadavatel uvedl požadavky na databázi v příloze č. 1 ZD – Technická specifikace v části: Základní požadavky a Požadavky na portál IDM.

Ad 18)
Zadavatel uvedl požadavky na vícefaktorovou autentifikaci v příloze č. 1 ZD – Technická specifikace v části: Základní požadavky.

Ad 19)
Zadavatel požaduje, aby dodavatel, který nabízí vlastní produkt, předložil certifikát pro osobu, která bude členem realizačního týmu. Zadavatel neuvádí přesnou podobu certifikátu, ale musí mít možnost certifikát ověřit.

Žádost o vysvětlení zadávací dokumentace č. 2 (obdržena dne 26. 04. 2018):

Dotaz č. 1:
V technické příloze zadávací dokumentace je uveden požadavek: "Plnou integrací je myšleno propojení IDM s využitím API daného IS pro plnou integraci. Cílem integrace IS je zabezpečení cílového IS a zabezpečení nakládání s oprávněním definovaným v business roli, případně v popisu systemizovaného místa. Dodavatel je povinen využít API daného systém pro integraci."

Rozumíme správně požadavku tak, že zadavatel zajistí u dodavatelů systémů, na které má být systém IDM napojen, standardizované API? Tzn. příprava těchto API, součinnosti a náklady na straně dodavatelů s tím související nejsou součástí požadovaného plnění v rámci projektu implementace IDM?

Dotaz č. 2:
Pokud dodavatel disponuje řešením IdM, které hesla k účtům neeviduje a je schopno za těmito účely využít napojení na Active Directory, což je rovněž požadováno v zadávací dokumentaci, případně pouze hesla předává do systémů, na které se integruje, naplní tímto způsobem řešení uchazeč požadavky ze zadávací dokumentace z části bezpečného úložiště hesel?

Pokud ne, tak prosíme o uvedení v čem konkrétně.

Dotaz č. 3:
V praxi jsou často uživatelé v rámci uvedených systémů spravovány přes nějaké standardizované adresářové služby jako např. Active Directory. Je možné uživatele uvedených OS spravovat přes tyto služby? Jsou mimo Active Directory požadovány nějaké jiné adresářové služby, které by měly být v rámci dodávky integrovány s IdM?

Dotaz č. 4:
V technické příloze zadávací dokumentace se objevuje pojem business role. Prosíme o bližší upřesnění tohoto pojmu. Jedná se o aplikační role opravňující přístup do dané aplikace, které je možné vázat na systemizovaná místa?

Dotaz č. 5:
Dále žádám o prodloužení lhůty na podání nabídek o min. 1 týden.

Informace zadavatele k žádosti č. 2 (poskytnuty dne 02. 05. 2018):

Ad 1)
Zadavatel nebude zajišťovat u dodavatelů systémů standardizované API. Dodavatel zajistí na vlastní náklad propojení s danými informačními systémy s upřednostněním propojení přes API.

Ad 2)
Pro vyjasnění dotazu ohledně nástroje IDM, který *využívá a poskytuje bezpečné úložiště hesel a privilegovaných účtů,* které je specifikované podle normy FIPS 140-2, lze syntakticky dekomponovat na přehlednější podobu:

Nástroj IdM:

1. *využívá bezpečné úložiště hesel a privilegovaných účtů,*
2. *poskytuje bezpečné úložiště hesel a privilegovaných účtů, které je specifikované podle normy FIPS 140-2.*

Tudíž:

A) Pokud dodavatelem navrhovaný nástroj/navrhované řešení neumí **ad 1.** a **ad 2.,** tak požadavek nesplňuje.

B) Pokud dodavatelem navrhovaný nástroj umí **ad 1.,** ale nikoliv **ad 2.,** tak požadavek nástroj IdM nesplňuje, ale vhodným doplněním funkcionality externím nástrojem k nástroji IdM může celkové řešení IdM požadavek splňovat.

C) Pokud dodavatelem navrhovaný nástroj/řešení neumí zajistit vazbu hesla s privilegovaným účtem, pak požadavek nesplňuje. Důvodem je, že takto předložený nástroj/řešení IdM neumožňuje splnit požadavek *identifikaci nesouladu uloženého hesla s heslem na koncovém zařízení.*

Cílem projektu IdM od zadavatele je dostat hesla privilegovaných účtů do bezpečného úložiště. V bezpečnosti zadavatel nepřipouští částečné plnění požadavku, protože bezpečnost je tak silná, jako je nejslabší článek. Tudíž pokud dodavatel má v plánu nabídnout řešení, které bude hesla evidovat v Active Directory, tak takové řešení požadavek nesplňuje. Tím by požadavek na bezpečné úložiště hesel privilegovaných uživatelů postrádal účel, pokud by zadavatel měl v cílovém provedení řešení

IdM hesla privilegovaných uživatelů ještě v jiném (a méně bezpečném) úložišti (jako např. Active Directory).

Ad 3):
Z pohledu zadavatele jsou za tzv. „nějaké jiné adresářové služby“ považovány následující uvedené adresářové služby:

- Microsoft Active Directory (Microsoft) – Zadavatel používá a plánuje nadále používat.
- Novell Directory Services (Novell eDirectory) – Zadavatel nepoužívá a neplánuje používat.
- Linux OpenLDAP (RedHat) - Zadavatel nepoužívá a neplánuje používat.
- Oracle Internet Directory (Oracle) - Zadavatel nepoužívá a neplánuje používat.
- Oracle Directory Services (Oracle) - Zadavatel nepoužívá a neplánuje používat.
- IBM Directory Server (IBM) - Zadavatel nepoužívá a neplánuje používat.
- Apache Directory (Apache Foundation) - Zadavatel nepoužívá a neplánuje používat.

Zadavatel hodlá specifikované operační systémy spravovat výhradně přes uznaný softwarový standard, kterým je Microsoft Active Directory.
Zadavatel ve výhledu 2 až 3 let neuvažuje o jiných adresářových službách, než je uznaný software standard Microsoft Active Directory.

Ad 4):
Zadavatel uvádí, že se jedná o soubor aplikačních rolí a přístupových oprávnění, tvořících business roli, vázaných k systematizovanému místu.

Ad 5):
Zadavatel neshledává důvod pro prodlužení lhůty pro podání nabídek.

V Ostravě dne 02. 05. 2018

Dopravní podnik Ostrava a.s.
Poděbradova 494/2
702 00 Ostrava, Moravská Ostrava
18

.....
Bc. Karla Holušová
hlavní specialista nákupu