VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE č. 03

dle ust. § 99 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále také „ZZVZ“)

K ZADÁVACÍ DOKUMENTACI A ZADÁVACÍM PODMÍNKÁM

dle ust. § 28 odst. 1 písm. a) a b) zákona **v nadlimitní veřejné zakázce na dodávky**

Zadavatel:	Metropolnet, a.s.		
Sídlo:	Mírové náměstí 3097/37, 400 01, Ústí nad Labem		
IČO / DIČ:	25439022 / CZ25439022		
Název zakázky:	**Metropolnet – dodávka AIS**		
Ev. číslo VVZ:	Z2018-023578	**Identifikátor ZP na profilu zadavatele:**	P18V00000131

Zadavatel obdržel dne 13. 08. 2018 žádost o vysvětlení zadávací dokumentace dle článku 5.4 zadávací dokumentace výše uvedené veřejné zakázky. Obdržené dotazy a odpovědi zadavatele jsou uvedeny níže.

Dotaz č. 01: *V kapitole 2. Základní požadavky na řešení, v podkapitole 2.1 Předmět realizace veřejné zakázky je uveden přehled stávajících aplikačních komponent.*

Na prvním místě je uveden IDM/správa uživatelů a oprávnění k výkonu agend, ve sloupci Záměr zadavatele je uvedeno Integrovat + rozšíření nebo nahrazení stávající komponenty.

a) Chápeme to správně, že by v případě nahrazení celé stávající komponenty IDM musel dodavatel nahradit celou stávající funkčnost IDM?

b) Může nyní zadavatel poskytnout detailní seznam funkcionalit, které musí dodavatel jiného IDM nahradit?

c) V mnoha dalších bodech zadávací dokumentace jsou odkazy na integraci s IDM. Znamená to tedy, že v případě změny IDM musí dodavatelé dalších komponent se integrovat na toto nové IDM?

Odpověď č. 01: K výše uvedenému dotazu zadavatel uvádí:

a) Ano, v případě nahrazení celé stávající komponenty IDM by musel dodavatel nahradit celou stávající funkčnost IDM.

b) Funkcionality IDM jsou nyní téměř výhradně vázány na celé prostředí MARBES PROXIO (Agendový systém, Volební systém, ISZR, evidence subjektů, …) a správu oprávnění jeho aplikací, včetně přiřazování funkčních rolí a oprávnění přístupu do ISZR pro konkrétní agendy a činnostní role. Integrace je nutná minimálně na tyto systémy: Datacentrum DC2 (import organigramu – dle toho zařazení do organizační jednotky v IDM), ActiveDirectory – synchronizace a vytváření účtů, ELISA (Spisová služba) – export účtů do tohoto systému. Skutečně detailní požadavky na IDM by bylo nutné zpracovat a zdá se vhodné vše popsat v rámci implementační analýzy (i za cenu případných víceprací).

c) Ano, znamená to, že v případě změny IDM musí být dodavatelé dalších komponent integrováni na toto nové IDM.

Dotaz č. 02: *Na str. 5 je uvedeno "Součástí předmětu plnění jsou i další dodávky a služby, které jsou nezbytné pro dosažení zadavatelem požadovaného cíle a o kterých dodavatel s ohledem na svoji odbornost a erudovanost měl nebo mohl vědět*

Má zadavatel nějaké další požadavky na dodávky a služby, které nejsou uvedeny v této zadávací dokumentaci?

Odpověď č. 02: Ne, zadavatel nemá další požadavky neuvedené v zadávací dokumentaci. Podle názoru zadavatele se však mohou vyskytnout požadavky spojené např. s konkrétním technickým řešením navrženým dodavatelem, které zadavatel nemohl předjímat – výše uvedené ustanovení se týká právě takových případů.

Dotaz č. 03: *V části Centrální správa identit, str. 7, bod 2: "IDM systém bude evidovat i občany přihlašující se na Portál občana. Tyto osoby nebudou synchronizovány ani s personálním systémem, ani do AD. V tomto případě se stane IDM nejen autorizačním nástrojem, ale i autentizační autoritou. Občané registrovaní pro přístup k portálu budou evidováni samostatně, odděleně od pracovníků úřadu. Jestliže budou uživatelé portálu evidováni v IDM, musí zde být uchována jejich identita (uživatelské jméno a heslo nebo jeho otisk). V případě vytvoření či změny hesla musí být definována určitá složitost hesla, např. heslo musí obsahovat malá písmena, velká písmena, číslice, minimálně délka hesla apod.*

Jakou složitost hesla Zadavatel požaduje?

Odpověď č. 03: Zadavatel požaduje hesla v rozsahu 10 znaků + malá/velká písmena, číslo nebo speciální znak (při zajištění 2FA není nutné silnější heslo). Z bezpečnostního hlediska by přihlašovací formulář Portálu občana měl hlídat, zda není na stránky veden „slovníkový“ nebo „bruteforce“ útok, aby bylo možné zamezit strojovému uhádnutí hesla (např. počet neúspěšných pokusů o přihlášení a dočasné zablokování účtu).

Dotaz č. 04: *V části Centrální správa identit, str. 8, bod 8: "Možnost sloučení více identit k jedné osobě. Chápeme tento požadavek správně, že pro občany, kteří se mohou zaregistrovat do Portálu občana různými způsoby, např. prostřednictvím mojeID musí být umožněno přidat ke stejnému občanovi ještě další způsob přihlašování, např. pomocí jména a hesla?*

Odpověď č. 04: Ano, dodavatel chápe požadavek správně za předpokladu, že platí níže uvedené:

Výše uvedená problematika se bude lišit dle konkrétního procesního případu:

- Registrací na přepážce úřadu (ověření identity zde):
  - JMÉNO, EMAIL, SILNÉ HESLO + NUTNOST 2FA PŘES GMS BRÁNU
- Elektronickým podáním s vícefaktorovým potvrzením:
  - Žádost doručená na podatelnu datovou schránkou, podepsaná elektronicky uznatelným podpisem občana a poté JMÉNO, EMAIL, SILNÉ HESLO + NUTNOST 2FA PŘES GMS BRÁNU
- Převzetím identity z MojeID – podle stupně ověření + 2FA
- Pomocí občanského průkazu s elektronickým čipem + 2FA

Je bezpečnostní otázka, zda jsou všechny výše uvedené typy ověření vnímány na stejném stupni ověření. Pokud ne, mělo by být aktivní vždy to nejvyšší možné ověření, kterým se občan identifikoval a ostatní přístupy s nižším stupně autentizace by měly být zrušeny (a občan by o tom měl být informován formou minimálně chybové hlášky, a u registrace nového typu zabezpečení).

Dotaz č. 05: *V části Centrální správa identit, str. 9, bod 12: "IDM musí podporovat 2FA (two-factor authentication) např. odesláním části hesla na e-mail a další části či potvrzení prostřednictvím SMS brány na mobil, zadání karty a jejího PIN."*

Předpokládáme, že na mobil budou zasílána hesla pouze pro externí uživatele (Portál občana), zatímco zaměstnanci úřadu se budou ověřovat vložením karty či tokenu a zadání pinu. Má již nyní Zadavatel k dispozici SMS bránu? Jestliže ano, prosíme o popis rozhraní pro komunikaci s touto bránou.

Odpověď č. 05: Ano, dodavatel chápe požadavek správně – na mobilní telefon budou zasílána hesla pouze externím uživatelům (např. uživatelé Portálu občana). Zadavatel nemá k dispozici služby SMS brány a předpokládá její pořízení z prostředků Zadavatele na základě diskuse s Dodavatelem (kompatibilita zařízení s jeho systémem), ať už jako hardware nebo jako službu operátora.

Dotaz č. 06: *V části Centrální správa identit, str. 9, bod 19: "Možnost „vedoucích" rolí v přidělování oprávnění a činnostních rolí pro své pracovníky ve dvou variantách 1. přímé zadání vedoucím, 2. požádání vedoucím a schválení v IT."*

Chápeme správně, že by v případě varianty 1. měli k IDM přímý přístup vedoucí pracovníci úřadu a mohli by tak přidělovat oprávnění sami sobě a svým podřízeným přímo v IDM? Oprávnění by tak přidělovali prostřednictvím profilů či na úrovni atributů a jejich hodnot? Oprávnění by mohli přidělovat pro všechny aplikace (včetně vlastního IDM), které má rovněž v sobě nastavitelné oprávnění přístupu?

Odpověď č. 06: Vedoucí odboru má mít oprávnění nastavit oprávnění pouze svým podřízeným a sám sobě (je to on, kdo nese za přidělená oprávnění zodpovědnost). Vždy bude mít možnost využít konzultace, či zadat požadavek na IT tak, aby mu s oprávněním pomohl a nastavil oprávnění za něj. U vybraných typů přihlášení (oprávnění vyššího řádu např. v rámci IDM) bude požadavek podléhat schválení IT. Musí tedy existovat předem definovaná sada možných oprávnění a definice role pro vedoucí odborů co ještě smí, a co již musí schvalovat IT.

Dotaz č. 07: *Správa čipových tokenů, str. 10. Chápeme ze zadání správně, že součástí plnění není dodávka čipových karet a USB tokenů, ani ovládací SW pro nahrání příslušného "mikrokódu" na kartu či USB token (certifikát, elektronický podpis, apod), že vše toto má již úřad k dispozici? Jedná se tedy o evidenci a integraci čipových karet a USB tokenů s IDM a AD?*

Odpověď č. 07: Ano, dodavatel chápe požadavek správně – součástí plnění není dodávka čipových karet a USB tokenů. Obslužný a uživatelský software k tokenům miniLector S EVO je software SecureSign (v 4.0) - http://www.ica.cz/Secure-Store pomocí jehož lze vydávat kvalifikované certifikáty a ukládat/zobrazovat další certifikáty uložené na kartě. Jedná se však o lokální „offline“ software, který neumožňuje evidovat tokeny „online“ na serveru a vést jejich životní cyklus (přihlášení k počítači pomocí AD, zneplatnění tokenu, vystavení certifikátu doménové autority, …) a neumožňuje integraci s IDM. Pro tyto účely musí existovat obslužný software pro správu karet, kterým zadavatel nyní nedisponuje a je předmětem dodávky v této veřejné zakázce.

Na základě výše uvedených dotazů zadavatel nemění text zadávací dokumentace. Předpokládá však, že dodavatelé zohlední výše uvedené vysvětlení ve své cenové nabídce.

Zadavatel zároveň sděluje, že ostatní informace v Zadávací dokumentaci jsou beze změny.

Vzhledem k charakteru vysvětlení zadávací dokumentace, které doplňují zadávací podmínky, zadavatel v souladu s ustanovením § 99 ZZVZ prodlužuje lhůtu k podání nabídek, **a to o 4 dny, tedy nová lhůta pro podání nabídek je stanovena na 27. 08. 2018 v 11:00 hodin**.

V Ústí nad Labem dne 20. 08. 2018