PRA HA
PRA GUE
PRA GA
PRA G

MHMPP092J7KW

(212)

Věc: Objednávka č. OBJ/IAP/31/03/00138/2020 „Nadstavbové řešení IDM MIDPOINT pro správu hesel"

OBJEDNATEL:

Hlavní město Praha

se sídlem:	Mariánské nám. 2, 110 01 Praha 1
pracoviště:	Jungmannova 35/29, 110 00 Praha 1
zastoupené:	Ing. David Vorlíček, pověřený řízením Odboru informatických aplikací Magistrátu hl. m. Prahy
IČO:	00064581
DIČ:	CZ00064581
bankovní účet:	[redacted]
kontaktní osoba:	

DODAVATEL:

AMI Praha a.s.

se sídlem:	Hanusova 29, 140 00 Praha 4
zastoupené:	Ing. Petr Šimek, místopředseda představenstva
IČO:	25715909
DIČ:	CZ25715909
kontaktní osoba:	Ing. Petr Šimek

(dále též „Smluvní strany")

Vážení,

ve smyslu § 27 a § 31 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, u Vás objednáváme odborné technické služby v rozsahu a za podmínek dále uvedených.

V souladu s občanským zákoníkem se akceptací této objednávky zakládá dvoustranný smluvní vztah mezi Objednatelem a Dodavatelem. Dodavateli tak vzniká povinnost realizovat předmět plnění v požadovaném rozsahu a jeho výsledky předat níže uvedenému zástupci Objednatele a Objednateli vzniká povinnost zaplatit Dodavateli dohodnutou smluvní odměnu.

1. **Předmět plnění:**

1.1 Předmětem plnění je nadstavbové řešení IDM MIDPOINT pro správu hesel. Detailní popis řešení je uveden v příloze 1 této Objednávky.

2. **Cena za předmět plnění:**

2.1. Uvedená cena za předmět plnění bez daně z přidané hodnoty (dále jen „DPH") je stanovena jako smluvní odměna ve výši 950 000 Kč (100 člověkodnů x 9 500 Kč/člověkoden). Tato cena je cenou maximální a nepřekročitelnou. V této částce jsou zahrnuty veškeré náklady Dodavatele vynaložené v souvislosti s realizací předmětu plnění, a to zejména náklady na

administrativní práce, na telekomunikace a poštovní styk v České republice a čas strávený na cestě za účelem konzultací při zpracování předmětu plnění na území hlavního města Prahy.

2.2. Dodavatel je plátcem DPH, DPH bude účtována podle platných právních předpisů. Cena včetně DPH činí 1 149 500 Kč.

3. Platební podmínky:

3.1. Cena za předmět plnění bude účtována Objednateli měsíčně na základě vystaveného výkazu plnění. Faktura musí být vystavena nejpozději do 10 dnů ode dne splnění předmětu objednávky. Součástí faktury musí být podrobný rozpis konkrétně uskutečněného plnění včetně počtu odpracovaných hodin (Výkaz plnění).

3.2. Konečná faktura bude vystavena po předání předmětu plnění (viz čl. 4.2.) (na základě „Protokolu o předání a převzetí předmětu plnění"). Dnem uskutečnění zdanitelného plnění bude den převzetí předmětu plnění.

3.3. Faktura bude vystavena na adresu sídla Objednatele uvedenou v záhlaví objednávky.

3.4. Faktura bude doručena na adresu pracoviště Objednatele uvedenou v záhlaví objednávky.

3.5. Splatnost faktury bude stanovena na minimálně 21 dnů.

3.6. Vystavená faktura musí mít veškeré náležitosti daňového dokladu ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a musí obsahovat minimálně tyto údaje:

a) označení Objednatele a Dodavatele, jejich sídla, jejich IČO a DIČ, bankovní spojení a údaj o zápisu v obchodním, živnostenském nebo obdobném rejstříku, včetně spisové značky,

b) předmět a číslo objednávky,

c) číslo faktury, den vystavení faktury, datum splatnosti, den uskutečnění plnění a fakturovanou částku,

d) základ daně (DPH), sazbu daně a její výši, razítko a podpis oprávněné osoby Dodavatele, stvrzující oprávněnost a formální a věcnou správnost faktury.

3.7. V případě, že faktura bude obsahovat nesprávné údaje nebo nebude obsahovat právními předpisy vyžadované údaje, je Objednatel oprávněn fakturu vrátit Dodavateli k opravě. Splatnost opravené faktury musí být stanovena opět na minimálně 21 dnů.

3.8. Objednatel uhradí cenu za předmět plnění bankovním převodem na účet Dodavatele, vedený u banky v České republice, specifikovaný v této objednávce. Ke splnění závazku Objednatele dojde odepsáním částky z účtu Objednatele.

4. Stanovený termín a místo plnění:

4.1. Objednatel je povinen oznámit Dodavateli přesné datum zahájení provádění předmětu plnění (dále jen „Datum zahájení prací") nejpozději do 3 dnů po uzavření této objednávky. Dodavatel je povinen začít s prováděním předmětu plnění do 3 dnů po datu zahájení prací.

4.2. Předmět plnění podle této objednávky je Dodavatel povinen předat k rukám [redacted] na adresu Jungmannova 35/29, 110 00 Praha 1, a to nejpozději do 30. 9. 2020.

5. Smluvní sankce:

5.1. Při prodlení Dodavatele s předáním předmětu plnění dle článku 1. této objednávky zaplatí Dodavatel Objednateli smluvní pokutu ve výši 0,5 % z maximální ceny předmětu plnění včetně DPH stanovené v článku 2. této objednávky za každý započatý kalendářní den prodlení až do řádného splnění této povinnosti.

5.2. Při porušení povinnosti Dodavatele zahájit provádění předmětu plnění podle článku 4.1 objednávky je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 0,1 % z maximální ceny předmětu plnění včetně DPH dle čl. 2. objednávky, nejméně však 1.000,- Kč (přiměřeně k předmětu plnění) včetně DPH za každý započatý den trvání prodlení.

5.3. Dodavatel je povinen smluvní pokutu uhradit na výzvu Objednatele do 5 dnů od jejího doručení.

5.4. Objednatel je oprávněn započíst si jednostranně vzniklou smluvní pokutu oproti odměně za provedení veřejné zakázky.

5.5. Zaplacením smluvních pokut dle této Objednávky není dotčeno právo Objednatele na náhradu újmy v části převyšující již uhrazenou smluvní pokutu.

6. Další podmínky:

6.1. Smluvní strany této objednávky výslovně souhlasí s tím, aby tato objednávka byla uvedena v Centrální evidenci smluv (CES) vedené hlavním městem Prahou, která je veřejně přístupná a která obsahuje údaje o jejích účastnících, předmětu, číselné označení této objednávky, datum jejího podpisu a její text.

6.2. Smluvní strany prohlašují, že skutečnosti uvedené v této objednávce nepovažují za obchodní tajemství ve smyslu § 504 občanského zákoníku a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoliv dalších podmínek.

6.3. Smluvní strany této objednávky výslovně sjednávají, že uveřejnění této objednávky v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) zajistí hl. m. Praha.

6.4. Dodavatel bere na vědomí, že Objednatel je povinen na dotaz třetí osoby poskytovat informace v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a souhlasí s tím, aby veškeré informace obsažené v této objednávce byly v souladu s citovaným zákonem poskytnuty třetím osobám, pokud o ně požádají.

6.5. Dodavatel je podle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů včetně prostředků poskytnutých z Evropské unie. Toto spolupůsobení je povinen zajistit i u svých případných subdodavatelů.

6.6. Dodavatel není oprávněn postoupit jakékoliv své pohledávky z této objednávky na třetí osobu bez předchozího písemného souhlasu Objednatele, a to ani částečně.

6.7. Pro případné spory smluvní strany sjednávají místní příslušnost obecného soudu Objednatele.

6.8. Tato objednávka může být měněna nebo zrušena pouze písemně, a to v případě změn objednávky číslovanými dodatky, které musí být podepsány oběma Smluvními stranami.

7. Lhůta k akceptaci objednávky

Dodavatel je povinen doručit akceptaci této objednávky Objednateli nejpozději do 14. 7. 2020, jinak tato nabídka na uzavření objednávky zaniká. Potvrzení objednávky nám zašlete zpět na adresu: Jungmannova 35/29, 111 21 Praha 1, datovou schránkou nebo na e-mail: [redacted]

Přílohy:

Příloha 1: Technický popis předmětu plnění

S pozdravem

Za Objednatele: 14 -07- 2020

Hlavní město Praha
Magistrát hl.m. Prahy
Jungmannova 35/29
111 21 Praha 1 /43/

[redacted]

Ing. David Vorlíček

pověřený řízením Odboru informatických aplikací MHMP

Dodavatel akceptuje tuto objednávku v plném rozsahu a bez výhrad.

V Praze dne 14.7.2020

Za Dodavatele:

[redacted]

Ing. Petr Šimek, AMI Praha a.s.

místopředseda představenstva

A) Základní požadovaná funkcionalita – přínos realizace:

1. Změna hesla pro externisty

Primárním cílem realizace je umožnit externím pracovníkům MHMP, kteří nemají přístup do interní sítě MHMP, změnit si heslo jemuž končí platnost pomocí ctrl-alt-del obrazovky pracovní stanice . Tito uživatelé nemohou ani do IdM, které je výhradně ve vnitřní síti. V současnosti je pro změnu hesla nutné, aby externista měl přístup do VPN a použil změnu hesla pomocí ctrl-alt-del obrazovky pracovní stanice v doméně. Externisté, kteří mají pouze email, si musejí měnit mailové heslo ve webové administraci emailu. Tímto však nejsou dotčená další hesla do případných další aplikací MHMP.

2. Změna hesla pro zaměstnance mimo síť MHMP

Zaměstnanec mimo síť MHMP je na tom stejně jako externista – jsou zaměstnanci, kteří mají vzdálený VPN přístup, ale neplatí to pro všechny. Přitom všichni používají vzdálený přístup k e-mailu.

3. Reset zapomenutého/expirovaného hesla

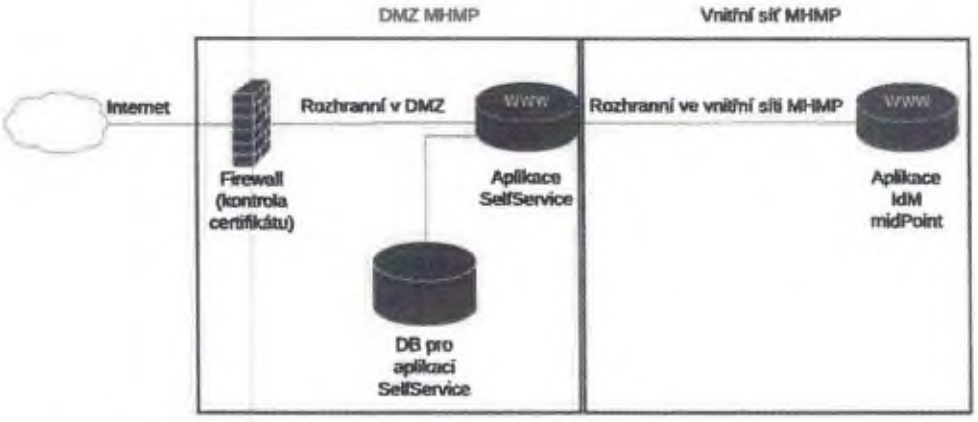
V případě, že uživatel heslo zapomene, je nutné, aby přímo nebo přes svého nadřízeného/garanta kontaktoval zaměstnanec/externista administrátora a ten jim nové heslo nastavil. Tímto se snižuje bezpečnost nového hesla, protože je potřeba ho předat sms nebo mailem. V případě přímého kontaktu je také vyšší riziko sociálního engineeringu.

B) Požadované technické řešení

Vystavení IdM do internetu je pro tyto účely nevhodná varianta. Došlo by tím k vystavení aplikace IdM, která řídí přístupy a oprávnění do všech systémů MHMP, útokům z internetu. Proto požadujeme vystavení jednoúčelové aplikace pro obsluhu hesel, která bude zabezpečená, nebude mít tak velká oprávnění a o resetu hesel bude komunikovat s aplikací IdM na jiném zabezpečeném rozhraní ve vnitřní síti. Tato aplikace zajistí samo-obslužnost změny hesla, správu vlastních osobních údajů a zároveň zabezpečení aplikace IdM midPoint.

1. Návrh architektury řešení

- Robustní aplikace odolná proti hacknutí:
  - sql injection, brute force, ukradená session, známé chyby.
- Postavená na známých a ověřených knihovnách (není vendor lock-in).
- Využití moderních technologií:
  - java + vhodné knihovny – jeden war soubor,
  - wicket – čistý html kód, modulární skládání web stránky,
  - hibernate – nezávislost na typu nebo verzi DB, odstínění DB specifikace.
- Moderní vzhled GUI:
  - přihlášení,
  - zobrazení profilu,
  - ochrana proti možnému hacknutí (aktualizace dat jiného profilu podvržením session),
  - responzivní GUI, zobrazitelné na všech typech zařízení.
- Nasazení na QA a instalační balíček.



2. Aplikace správy hesel

Požadovaná webová aplikace bude veřejně dostupná na internetu. Aplikace bude uživatelům umožňovat změnit si heslo do sítě MHMP, zobrazit profil aktuálně přihlášeného uživatele a resetovat zapomenuté heslo.

Vybraná data uživatelů budou uložena spolu se zašifrovaným heslem v tabulce profilů externistů, která bude plněna ze strany IdM. Zpět z tabulky si IdM načte změněné heslo uživatele a následně provede synchronizaci do ostatních napojených aplikací. Výběr osobních údajů je možný z údajů dostupných v objektu uživatele v aplikaci IdM midPoint.

3. Požadavky na aplikaci

Aplikace bude sloužit pro změnu hesla uživatelů zavedených v IdM. Uživatel si v SelfService změní heslo s kontrolou Passwod Policy (uloženo SHA-256, nikdy to není plaintext), IdM načte změnu a propaguje dál do připojených aplikací. Aplikace zobrazuje základní údaje o profilu uživatele v režimu read-only. Password Policy bude vycházet z aktuálně platné směrnice MHMP.

4. Případy užití

Jde o aplikaci, která umožní využít základní funkcionalitu IdM mimo síť MHMP. Aplikace umožní jednoduché zobrazení vlastního profilu, změnu hesla a reset zapomenutého hesla a to pro zaměstnance i externisty MHMP. Uživatelé se do aplikace přihlásí jménem a heslem z Active Directory MHMP.

a. Zobrazení profilu

Uživateli se po přihlášení do aplikace a volbě *Můj profil* zobrazí základní osobní údaje, které o něm jsou v IdM evidovány. Pokud některé z údajů nesouhlasí, může iniciovat jejich změnu (kanály mimo aplikaci SelfService).

b. Změna hesla

Uživateli se po přihlášení do aplikace a volbě *Změna hesla* zobrazí formulář pro zadání nového hesla. Nové heslo musí uživatel zadat pro potvrzení 2x. Jsou kontrolovány shodné politiky pro nastavení hesla jako v IdM. Po vyplnění nového hesla a odeslání formuláře je nové heslo synchronizováno do IdM a z něj do všech online připojených systémů. O změně hesla přijde uživateli notifikace z centrálního IdM.

c. Zachování funkce ctrl-alt-del

Pro uživatele v doméně je zásadní funkce zachování možnosti změny hesla na své pracovní stanici pomocí obrazovky po stisku ctrl-alt-del. Toto bude řešeno návrhem, implementací a instalací agenta na servery AD, který bude tyto změny hesla propagovat do IdM. IdM pak takto změněné heslo bude propagovat do všech ostatních systémů standardním způsobem.

d. Reset hesla s účastí administrátora

Uživatel kontaktuje administrátora IdM na straně MHMP kanálem mimo aplikaci správy hesel (telefonicky, e-mailem, přes nadřízeného apod.). Administrátor uživateli nastaví v IdM heslo, které je v tuto chvíli funkční pouze jako „jednorázové" heslo, které je odesláno e-mailovou notifikací uživateli, který zatím zůstává zablokovaný. Primárně jde zde tedy o zachování stávajícího procesu s tím, že je zaručena změna hesla po jeho předání koncovému uživateli. Do aplikace pro správu hesel se v tomto procesu nepřistupuje.

e. Varianta bez účasti administrátora

Pro možnost resetu hesla bez účasti administrátora je nutné autorizovat uživatele jiným způsobem než ověřením znalosti jeho hesla. Navržené jsou 2 způsoby, a to ověření pomocí vlastnictví předem zadané emailové schránky a ověření vlastnictvím předem zadaného telefonního čísla.

- **Varianta přes e-mail:**
  - Uživatel použije volbu Reset hesla – email, která bude dostupná z úvodní obrazovky ještě před přihlášením.
  - Po výběru této volby bude uživatel vyzván k zadání e-mailové adresy. Půjde o rezervní (soukromou) emailovou adresu, která byla před tím zadána do IdM.
  - V případě nenalezení zadané e-mailové adresy bude uživatel upozorněn a žádná další akce nebude provedena.
  - Pokud bude e-mailová adresa v databázi aplikace pro správu hesel (synchronizována s IdM) nalezena, bude uživateli na tuto e-mailovou adresu odeslán unikátní jednorázový odkaz na reset hesla. Tento odkaz bude přístupný z veřejného internetu a umožní změnu hesla uživatele, kterému byl zaslán. Odkaz bude platný pouze 30 minut.
  - Samotná změna hesla již probíhá stejně jako v případě použití standardní volby Změna hesla, která je popsána výše.
- **Varianta přes SMS**
  - Uživatel použije volbu Reset hesla – SMS, která bude dostupná z úvodní obrazovky ještě před přihlášením.
  - Po výběru této volby bude uživatel vyzván k zadání svého telefonního čísla.
  - V případě nenalezení zadaného telefonního čísla bude uživatel upozorněn a žádná další akce nebude provedena.
  - Pokud bude telefonní číslo v databázi aplikace pro správu hesel (synchronizována s IdM) nalezeno, bude uživateli na toto číslo odeslán unikátní jednorázový kód pro reset hesla. Tento kód bude platný pouze 30 minut. Kód bude moct uživatel zadat použitím volby „opsání kódu" ze stránky Reset hesla – SMS. Po potvrzení kódu uživatelem a

ověření platnosti kódu aplikací bude uživatel přesměrován na obrazovku pro změnu hesla.

- Samotná změna hesla již probíhá stejně jako v případě použití standardní volby Změna hesla, která je popsána výše.

- **Navrhovaný způsob zabezpečení aplikace**
  - Rizika útoků typu brute force, dictionary attack nebo password spray budou mitigována existujícími prostředky ve správě MHMP, které jsou na aplikaci nezávislé, jako je ochrana uzamčení po několika pokusech a další bezpečnostní řešení (F5 WAF, CheckPoint IPS).

C) Požadovaná etapizace realizace

Požadujeme nasazení a rozvoj aplikace etapizovat, aby bylo možné řídit její rozvoj na základě empirických zkušeností z aktuálního používání uživateli:

1. **Etapa 1**

V 1. etapě bude zachován současný proces resetu zapomenutého hesla, jelikož jde zatím o okrajovou záležitost. Pro vyřešení řízení a kontroly změn hesla pro externisty bude nasazena aplikace pro správu hesel v minimalistické konfiguraci bez resetu hesla.

2. **Etapa 2**

Pro zlepšení kontroly nad politikou hesel v celém prostředí MHMP bude v 2. etapě nasazen agent pro synchronizaci hesla do IdM z AD. Tím se zachová pro uživatele jejich současný pracovní postup změny hesla přes obrazovku ctrl-alt-del a zároveň bude nové heslo propagováno do všech systémů, kam má uživatel přístup.

3. **Etapa 3**

Pokud bude potřeba automatizace procesu resetu hesla stále aktuální, navrhujeme v této fázi implementovat a nasadit reset hesla bez administrátora ve variantě přes email. Součástí této etapy by měla být i kampaň na straně MHMP s účelem shromáždit záložní emaily pro všechny uživatele. Tyto emaily bude možné zadávat přímo do IdM, nebo hromadně importovat z *.csv souboru.

4. **Etapa 4**

Pokud bude zbývat větší množství uživatelů, kteří nebudou mít možnost použít záložní email, a budou mít zájem o použití resetu hesla bez administrátora pomocí SMS, navrhujeme v poslední etapě implementovat a nasadit variantu přes SMS.

Součástí této etapy by měla být i kampaň na straně MHMP s účelem posbírat telefony pro všechny uživatele. Tyto telefony je možné zadávat přímo do IdM, nebo hromadně importovat z *.csv souboru.

D) Volitelná rozšíření

- Snadná rozšiřitelnost aplikace – odladění a příprava pro snadný budoucí rozvoj aplikace - např. možnost aktualizovat některé položky (kontaktní telefon, email, ...).
- Vizuální online kontrola hesla proti definovaným politikám, povolení uložení hesla až po splnění politik.