

Objednatel:	Hlavní město Praha zastoupené Mgr. Jiřím Károlým, ředitelem odboru informatických činností MHMP	Poskytovatel:	AMI Praha a.s.
sídlo:	Mariánské nám. 2/2 110 01 Praha 1	sídlo:	Hanusova 29 140 00 Praha 4
IČO:	00064581 DIČ: CZ00064581	IČO:	25715909 DIČ: CZ25715909
kontaktní osoba:	Vlastislav Dočkal	kontaktní osoba:	Václav Uhlíř
tel. spojení:		tel. spojení:	
fax:		fax:	
e-mail:		e-mail:	

Na základě Smlouvy o zajištění maintenance, upgrade a rozvoje stávajícího informačního systému Identity Managementu, ze dne 10.5.2023, účinné dne 11.5.2023 (dále jen „**Smlouva**“) s číslem INO/40/04/003861/2023, se realizačnímu týmu poskytovatele ukládá dodávka a realizace Služeb na objednávku dle článku 3.1.4 Smlouvy.

1. Předmět Služeb na objednávku vč. požadovaných výsledků plnění Služeb na objednávku:

Předmětem služeb na objednávku jsou činnosti definovány a blíže specifikovány v nabídce dodavatele ze dne 16.4.2025, která je přílohou této objednávky a zahrnují následovně:

Předmětem nabídky je úprava systému IDM a Self-service v souladu s metodickým pokynem Magistrátu hl.m. Prahy, který směřuje k budoucímu splnění standardu NIS. Úpravy zahrnují zavedení jednotného místa pro změnu hesla, což povede k úpravám procesů. Dále se zvýší požadavky na složitost hesel a přidá se nová kategorie požadavků pro administrátorské účty.

ÚPRAVA SYSTÉMU SELF SERVICE

Vzhledem k tomu, že Self-Service se má stát jediným místem pro změnu, je potřeba posílit jeho dostupnost.

Infrastrukturní část

Je nutné vytvořit a ověřit infrastrukturní schéma pro zajištění vysoké dostupnosti aplikace Self-Service. Tento proces zahrnuje instalaci nové verze systému Self-Service a úpravu stávající instalace tak, aby splňovala požadovaný standard. Možné bude i navýšení kapacity stávajícího serveru. Dále je potřeba zajistit přístupnost a viditelnost serveru do internetu prostřednictvím Load Balancer (LB) adresy. Následně bude vytvořen load balancer, který bude přesměrovávat provoz na node1 a v případě jeho výpadku na node2 v režimu activepassive. Pro databázovou část aplikace bude implementováno řešení vysoké dostupnosti pomocí Oracle DataGuard v shodném duchu. Také bude zajištěna integrace logů aplikace s centrálním log managerem a monitoring obou nodů.

Implementační část – databáze

Úprava databáze pro možnost identifikace administrátorských účtů.

Implementační část – aplikace

Do aplikace bude přidáno podrobnější logování pro běžné akce v rámci systémů a zajištění detailnější informace o aktérově a další auditní informace. Uplatnění nových standardů hesla pro stávající obrazovku, přidání obrazovky pro administrátory a logika zobrazování této obrazovky. Obrazovka obsahuje realtime

validaci, zda heslo plní podmínky. Aplikace zámek pro mnohonásobné pokusy o nepovedené žádosti z určité IP adresy. Zapomenuté heslo pro interní zaměstnance bude systém odesílat na dedikované uživatele.

ÚPRAVA SYSTÉMU IDM

Password L1 support process

Vytvoření nové role pro operátora L1: Vytvoření role pro operátora L1, který bude mít omezený přístup k funkcím systému IDM. Tato role poskytne operátorovi možnost vidět uživatele, změnit heslo, odemknout účet a vidět PIN pro ověření uživatele.

Nový atribut pro L1 a admina: Implementace nového atributu, který bude viditelný pouze pro L1 a administrátora. Tento atribut obdrží každý uživatel při vytvoření svého účtu.

Přejímání statusu "locked" z AD do IDM: Zajištění synchronizace mezi AD a IDM, kdy změna statusu uzamčení účtu v AD bude reflektována v IDM a naopak. Tato synchronizace umožní odemykání účtu v AD prostřednictvím IDM.

Propagace zákazu změny hesla do AD: Zavedení mechanismu, který zajistí, že jakýkoliv zákaz změny hesla v IDM bude automaticky propagován do AD.

Úprava role uživatele/externisty: Úprava role uživatele a externisty tak, aby v IDM nebyla možnost měnit heslo, čímž se zajistí, že tyto změny budou řízeny centrálně.

Úprava konektoru a konfigurace pro přenos.

Monitoring

Tvorba účtu pro autorizaci monitoringu: Vytvoření specializovaného účtu s autorizací pro čtení stavu autorizačních úloh. Tento účet bude mít přístup na REST rozhraní pro získání potřebných informací o stavu.

Zařazení checku pro synchronizační úlohy: Zavedení kontrolního mechanismu (checku) prostřednictvím REST do monitorovacích služeb pro úlohy synchronizace self-service a úkoly pro připomenutí změny hesla (password remind tasks).

Zahrnutí auditních záznamů do logů: Zajištění, že výstupy auditních záznamů budou zařazeny do centrálního logu, který bude koordinován s OICT pro další analýzu a vyhodnocování.

Nové politiky hesla

Replikace pravidel nové směrnice: Implementace pravidel nové směrnice týkající se politiky hesel v souladu s nastavením Self-Service (SS). To zahrnuje například pravidla pro složitost hesel, minimální délku, expiraci hesel apod.

Přidání úlohy pro expiraci hesla: Zavedení nové úlohy, která bude uživatelům informovat o blížícím se vypršení platnosti hesla. Uživatelé obdrží upozornění 30 dnů před expirací, následně 14, 7, 3 a 1 den před expirací.

Úprava šablony e-mailů pro informování o expiraci hesla: Aktualizace výstupů z úkolu pro informování uživatelů o expiraci hesla, včetně přechodu na novou šablonu e-mailů pro efektivnější komunikaci.

2. Požadovaný termín zahájení a případně ukončení poskytování Služeb na objednávku:

Termín plnění do 45 pracovních dní od potvrzení objednávky

3. Stanovení akceptačních kritérií:

Dle smlouvy č. INO/40/04/003861/2023 čl. 12 Smlouvy bude akceptační procedura probíhat písemným schválením akceptačního protokolu.

Akceptace je závislá na odevzdání dokumentace, která bude pokrývat již zmíněná témata/kapitoly.

Jestliže jednotlivé Dílčí plnění splní akceptační kritéria, poskytovatel se zavazuje nejpozději v pracovní den následující po ukončení akceptačních procedur umožnit Objednateli toto Dílčí plnění převzít a Objednatel se zavazuje k jeho převzetí nejpozději do deseti (10) pracovních dnů. Smluvní strany se zavazují o tomto převzetí

sepsat akceptační protokol.

Akceptační scénáře

- Akceptace bude provedena po skončení „pilotního provozu“.

4. Objednatelem předpokládaný rozsah Služeb na objednávku a cena za Služby na objednávku:

665.600 Kč bez DPH (805.376 Kč s DPH)

Cena za realizaci Díla na objednávku bude zaplacená vždy po akceptaci dílčího plnění způsobem dle čl. 12 Smlouvy, a to na základě faktury vystavené Poskytovatelem. Poskytovatel předloží Objednateli spolu s fakturou písemně podepsaný akceptační protokol příslušné Služby na Předmětovou objednávku.

Poskytovatel akceptuje tuto Objednávku v plném rozsahu a bez výhrad.

Za Objednatele:	Za Poskytovatele:
V Praze dne	V Praze dne
Mgr. Jiří Károly oprávněná osoba v záležitostech smluvních dle Smlouvy	Ing. Petr Šimek oprávněná osoba v záležitostech smluvních dle Smlouvy