



Úpravy Self Service pro změnu PIN pro komunikaci se supportem pro odblokování a reset hesla

PRA	HA
PRA	GUE
PRA	GA
PRA	G

Platnost nabídky: 31 dní



Technické a obchodní informace uvedené v tomto dokumentu jsou výhradním majetkem společnosti AMI Praha a.s. Tento dokument je vytvořen výhradně pro účely Zadavatele, a proto tento materiál ani informace v něm obsažené nesmí být poskytnuty nebo vyzrazeny jiné straně nebo použity pro jakékoliv jiné účely bez předchozího písemně potvrzeného souhlasu společnosti AMI Praha a.s.

Nabídku zpracovali:

Dominik Souček, solution architect

Tereza Schertlerová, key account manager

1 MANAŽERSKÉ SHRUTÍ

Na základě podepsané smlouvy č. INO/40/04/003861/2023 o zajištění maintenance, upgrade a rozvoje stávajícího informačního systému identity managementu ze dne 9.5.2023 si vám dovoluujeme předložit nabídku změnového požadavku, které se týká úprav stávající aplikace self-service pro změnu PIN pro komunikaci se správou hesel s plánovanou aktivací k 16.6.2025.

Tato nabídka spadá dle výše uvedené smlouvy do oblasti Předmětové objednávky.

OBSAH

1	MANAŽERSKÉ SHRUTÍ.....	3
2	PŘEDMĚT NABÍDKY	5
2.1	ÚPRAVA SYSTÉMU SELF SERVICE	5
2.1.1	Implementační část – databáze.....	5
2.1.2	Implementační část Self-Service	5
2.1.3	Implementační část konektor Self-Service.....	6
2.1.4	Implementační část IdM	6
2.2	NAPOJENÍ ONLINE SYSTÉMU ASPI PŘES ACTIVE DIRECTORY A JEHO ZAŘAZENÍ DO IDM PROCESŮ	6
3	VEDENÍ PROJEKTU	8
3.1	HARMONOGRAM	8
3.2	SOUČINNOST ZADAVATELE	8
4	CENOVÁ NABÍDKA	10
4.1	REALIZACE PROJEKTU	10
4.2	IDENTIFIKAČNÍ ÚDAJE	12
5	ZÁVĚR.....	13

2 PŘEDMĚT NABÍDKY

Nabídka se zaměřuje na úpravy systému Self-service v souladu s metodickým pokynem Zadavatele, který směřuje k budoucímu splnění standardu NIS. Úpravy zahrnují změny systému Self Service pro poskytnutí možnosti změny PIN obdobným způsobem jako je to u hesla. Zároveň obsahuje změnu uživatelského rozhraní pro správu hesel v IdM.

2.1 ÚPRAVA SYSTÉMU SELF SERVICE

2.1.1 Implementační část – databáze

Úprava databáze pro možnost ukládání PIN.

2.1.2 Implementační část Self-Service

Do aplikace bude na obrazovce s parametry přidána možnost pro změnu PIN. Viz obrázek



PIN bude měněn na nové obrazovce a po jeho dvojím zadání viz obrazovka níže:

ZMĚNA PIN

Váš nový pin pro komunikaci s helpdesk service-desk pro reset hesla či odemknutí účtu.
PIN po změně bezpečně uchovejte. .

Vyčkejte na potvrzení změně PINu na email, v případě chybějícího potvrzení se obraťte na správce systému IDM.

Nový PIN

Nový PIN znovu

Změnit PIN

PIN bude v šifrované formě, čitelné pouze IdM stranou uloženo do databáze, kde ho IdM v rámci live synchronizace zkonsumuje.

2.1.3 Implementační část konektor Self-Service

Konektor bude rozšířen o přenos atributu PIN, jeho rozšifrování a následné uložení do atributu uživatele.

2.1.4 Implementační část IdM

IdM na změnu PIN bude reagovat zasláním potvrzení uživateli o úspěšné změně.
Mechanismus je zde z důvodu omezené platnosti změny, která je zároveň bezpečnostním opatřením.

Do rozhraní pro reset hesla bude uživatelům přidán nový sloupec označující datum expirace aktuálně platného hesla.

2.2 NAPOJENÍ ONLINE SYSTÉMU ASPI PŘES ACTIVE DIRECTORY A JEHO ZAŘAZENÍ DO IDM PROCESŮ

V rámci rozšiřování identity managementu (IDM) budeme realizovali napojení online systému ASPI skrze Active Directory (AD). Toto propojení umožňuje jednotnou správu uživatelských účtů a jejich přístupových práv napříč celým prostředím. Uživatelské identity jsou řízeny centrálně přes AD, přičemž přiřazení oprávnění do systému ASPI je odvozeno na základě členství uživatele v AD skupinách.

Součástí integrace bude také:

- Tvorba garantských rolí: V rámci IDM budou definovány garantské role – garant ASPI a technický garant ASPI s příslušnými oprávněními
- Katalog rolí pro systém ASPI: Pro zvýšení přehlednosti a automatizace správy přístupů bude vytvořen katalog rolí, ve kterém jsou jednotlivé role kategorizovány podle typových činností a přístupových práv v systému ASPI. Tento katalog bude publikován v IDM a bude dostupný uživatelům i garantům.
- Další utilizace systému ASPI v IDM:

Automatizované přidělování rolí: Na základě organizační struktury, pracovního zařazení nebo typu uživatele (např. interní, externí) dochází k automatickému přiřazování základních oprávnění.

Workflow pro žádosti o role: Uživatelé mohou žádat o přístup do systému ASPI nad rámec automatického přiřazení prostřednictvím IDM portálu. Tyto žádosti podléhají schvalovacímu workflow, které zohledňuje pravidla stanovená guaranty.

3 VEDENÍ PROJEKTU

3.1 HARMONOGRAM

Níže je uveden orientační harmonogram prací, který může být po dohodě se Zadavatelem ještě upřesněn.

Krok	Popis	Pracovní dny
A	Zahájení projektu – objednávka Zadavatele	0
B	Realizace	A + 21
C	Interní testování	B + 5
D	Akceptační procesy	C + 10
		36

3.2 SOUČINNOST ZADAVATELE

Konkrétní technické požadavky

- Dodání notifikační zprávy pro potvrzení změny PIN.
- Zajištění VPN přístupu do všech prostředí pro celý projektový tým.

Obecné principy součinnosti

- Poskytnutí potřebných podkladů pro realizaci projektu. Podklady musí být dodány v odpovídajícím termínu a formě, které budou před započítím prací společně domluveny a schváleny Dodavatelem.
- Určení a dostupnost jedné odpovědné a kompetentní osoby na straně Zadavatele.
- Schvalování výstupů a stavu projektu v termínech pro to určených a dále testování funkčních částí projektu bez zbytečných odkladů.
- Poskytování konzultací při potřebě konkretizování nejasných bodů zadání, analýzy a v průběhu celého projektu.
- Zajištění kapacit k provedení akceptačních testů.
- Dodávat informace k projektu úplně a včas.

Reakční doby poskytování součinnosti

Pro dodržení termínů projektu je nezbytné, aby byla součinnost ze strany Zadavatele poskytovaná v co nejkratším čase. Zejména v úvodní fázi projektu hrozí největší riziko zpoždění. Obecně v průběhu projektu očekáváme splnění požadavku na součinnost do pěti pracovních dnů od vyžádání, jinak bude požadavek eskalován dle dohodnutého procesu, pokud by byly ohroženy termíny projektu.

Akceptační procedura

Akceptace se řídí smluvním vztahem číslo INO/40/04/003861/2023 kapitola 12.

4 CENOVÁ NABÍDKA

4.1 REALIZACE PROJEKTU

Veškeré ceny jsou uváděny v Kč bez DPH. MD sazba je dle smlouvy 12.800 Kč / MD.

Položka	Počet MD	Cena v Kč
Frontend-Tlačítko a detail uživatele-Obrazovka pro změnu PIN	2	25 600
Backend-Šifrování a update v DB	1	12 800
Midpoint-Notifikace po změně PIN	1	12 800
Midpoint-Konektor	2,5	32 000
Midpoint-Resource mapping	0,5	6 400
SelfService-Úprava a doplnění notifikací o chybových stavech	1	12 800
SelfService-Info o vypršení hesla operátorům	1,5	19 200
SelfService-Info o změně hesla v SS	1	12 800
SelfService-FIX javascript knihoven z roku 2019	1,5	19 200
Napojení systému ASPI	2,5	32 000
Test	2	25 600
Nasazení	2	25 600
PM	3	38 400
Celkem	21,5	275 200 Kč

- Doplnění informací k položce: „Frontend – Tlačítko a detail uživatele – Obrazovka pro změnu PIN”
- SelfService aplikace bude obsahovat novou obrazovku pro změnu PIN s validací délky a nové tlačítko pro změnu PIN na obrazovce detailu uživatele.
- Doplnění informací k položce: „Backend – Šifrování a update v DB” - PIN je nejdříve zašifrován a poté uložen do rozšířeného schématu databáze.
- Doplnění informací k položce: „Midpoint – Notifikace po změně PIN” – Po úspěšném načtení nového PIN kódu do systému Identity Management (IdM) MidPoint je automaticky spuštěn notifikační workflow, který uživatele informuje o tom, že jeho PIN byl uložen a evidován v systému. Notifikace je zasílána prostřednictvím e-mailu, jehož obsah je definován v šabloně uložené v MidPoint repozitáři (soubor .xml nebo .html podle konfigurace). Odeslání je zajištěno pomocí standardního mechanismu MidPoint notifikací, který využívá konfigurovaný SMTP server. Z technického hlediska je spuštění

notifikace vázáno na změnu hodnoty atributu extension/PIN. Trigger je nastaven v rámci schématu notifikační politiky (policyRule), která reaguje na úspěšné uložení nové hodnoty. Díky tomuto mechanismu má uživatel jistotu, že změna proběhla korektně, zároveň je možné změnu auditovat.

- **Doplnění informací k položce: „Midpoint-Konektor” a k položce: „Midpoint-Resource mapping”** - IdM konektor pro SelfService aplikaci načítá přes rozšířené schéma uživatele PIN z aplikace a podporuje smazání PIN v aplikaci po nastavení nového kontrolního atributu deletePinControl. IdM PIN po načtení ze SelfService uloží do detailu uživatele v IdM a následně v aplikaci smaže. K PINu je možné nastavit jiné časové omezení platnosti než k zašifrovanému heslu uživatele.
- **Doplnění informací k položce: „SelfService – Úprava a doplnění notifikací o chybových stavech”** - Při nekonzistenci některých funkcí aplikace tuto skutečnost detekovala a zapsala do aplikačního logu, nicméně nebyl důvod k ní přiřazovat mailovou notifikaci na uživatele. V současné době důležitost aplikace SelfService vzrostla a hraje klíčovou roli v samostatné správě přístupových údajů uživatelů, a proto je zásadní, aby poskytovala jasnou a spolehlivou zpětnou vazbu při každé akci. Po review aplikačního kódu a jeho opravě se nyní uživatelé o **všech** chybových stavech dozví obecnou zprávou **"Omlouváme se, ale akce bohužel skončila chybou aplikace."** spolu s uvedením konkrétní funkčnosti, která selhala:

"PIN se nepodařilo změnit."

"Heslo se nepodařilo změnit."

"Odeslání emailu pro arnost.starosta@ami.cz se nezdařilo."

- **Doplnění informací k položce: „SelfService - Info o vypršení hesla operátorům”** - Operátoři nyní vidí na přehledových obrazovkách pro interní zaměstnance, dohodáře a zastupitele informace o nejbližším vypršení hesla, a to buď dočasně nastaveného operátorem, nebo běžného, nastaveného uživatelem. Operátoři již nemají možnost přegenerovat PIN, nastavují ho uživatelé v SelfService aplikaci.
- **Doplnění informací k položce: „SelfService - Info o změně hesla v SS”** – Implementace úpravy formátování informační zprávy o úspěšné změně hesla v uživatelském rozhraní aplikace za účelem zlepšení její viditelnosti a důležitosti pro koncové uživatele. Identifikace příslušných stylů a CSS tříd. Testování zobrazení napříč různými prohlížeči a kontrola responzivního chování na mobilních zařízeních.
- **Doplnění informací k položce: „SelfService-FIX javascript knihoven z roku 2019”** - V rámci upgrade IDM byla řešena kompatibilita s novou verzí MP a přechod na novou verzi Javy. Upgrade midpoint nezahrnoval v nabídce změny týkající se SS komponenty. V původním projektu SS byl řešen také separátně. V rámci upgrade tedy nebyl řešen front end aplikace. Projekt metodiky hesla a řešení bezpečnostních politik ukázal, že aplikace obsahuje "vložené" knihovny mimo centrální správu MAVEN, nicméně nebyl prostor ve scope a vzhledem k termínu řešit. Vzhledem k plánovaným bezpečnostním testům a změně využití Self-Service tato skutečnost byla vyhodnocena jako riziko a nutné označena k úpravě. V rámci projektu pin byl SS aktualizován na nejnovější verze knihoven a přepracován jeho frontend a část obsahující vložené knihovny přesunuta do centrální správy.
- Napojení systému ASPI – viz kapitola 2.2

4.2 IDENTIFIKAČNÍ ÚDAJE



Fakta o společnosti

Název společnosti	AMI Praha a.s.
Doba působení na trhu	od roku 1996
Počet pracovníků	70
Obrat	290 milionů Kč (za rok 2024)
Sídlo	Hanusova 29, 140 00 Praha 4
Poštovní adresa	Pernerova 697/35, 186 00 Praha 8
Právní forma	akciová společnost
IČO	25715909
DIČ	CZ25715909
Obchodní rejstřík	zapsána v OR u MS v Praze, oddíl B, vložka 5673
Statutární zástupci	Ing. Petr Urban, předseda představenstva
	Ing. Petr Šimek, místopředseda představenstva
Bankovní spojení	Československá obchodní banka, a. s.
	č. ú.: 150823774/0300
Telefon	(+420) 604 444 848
E-mail	obchod@ami.cz
URL	www.ami.cz



Hlavní kontaktní osoba

Jméno a příjmení	Tereza Schertlerová
Pozice/funkce	key account manager
Telefon	
E-mail	
Adresa	

5 ZÁVĚR

Děkujeme za vaši poptávku a věříme, že vás naše nabídka zaujala. V případě potřeby doplnění jsme vám k dispozici telefonicky či e-mailem na níže uvedené adrese. Nabízené řešení s vámi rádi prodiskutujeme i osobně a následně nabídku upravíme dle vašich potřeb.

Tereza Schertlerová
key account manager

