

Určeno všem dodavatelům

Vyřizuje / linka: Kodýtková/ +420 378 037 535
Naše spis. značka: PTK/02/2025/PMDP
Naše č.j.: 371/ÚGŘ/ZKO/PMDP/2025

Plzeň 20. 3. 2025

Oznámení o předběžných tržních konzultacích

Implementace systému vícefaktorového ověřování uživatelů (Multi Factor Authentication - MFA) v PMDP

1. ÚVOD

Plzeňské městské dopravní podniky, a.s., se sídlem Denisovo nábřeží 920/12, Východní Předměstí, 301 00 Plzeň, IČO: 25220683, zapsané v obchodním rejstříku vedeném Krajským soudem v Plzni, oddíl B, vložka 710 (dále jen „PMDP“) jsou provozovatelem městské hromadné dopravy v Plzni a přilehlém okolí a **v současné době zvažují možnost implementace systému vícefaktorového ověřování (MFA) do domény Active Directory, VPN, RDP a případných dalších on-premise aplikací.**

2. ÚČEL KONZULTACE

PMDP se rozhodly vést tyto předběžné tržní konzultace (dále též jako „PTK“), aby získaly informace o dostupných řešeních vícefaktorového ověřování (MFA) na trhu, které by splňovaly naše požadavky na ochranu přihlašování uživatelů a administrátorů do domény Active Directory, VPN a případně dalších on-premise aplikací. Účelem těchto PTK je zvýšení transparentnosti případného budoucího výběrového řízení a získání relevantních a objektivních informací o možnostech trhu tak, aby PMDP mohlo následně optimálně nastavit podmínky pro výběr MFA řešení.

Cílem předběžné tržní konzultace je zejména získání relevantních informací pro rozhodnutí vedení PMDP o nákupu a implementaci MFA systému. Podrobné podmínky případné realizace zakázky budou vymezeny v zadávací dokumentaci až na základě výsledků těchto PTK.

3. FORMA A PRŮBĚH PŘEDBĚŽNÝCH TRŽNÍCH KONZULTACÍ

Účast v předběžných tržních konzultacích je **otevřená**.

Oznámení o zahájení PTK bude uveřejněno na profilu zadavatele (PMDP) <https://zakazky.pmdp.cz/vz00000417> a účastnit se tak mohou všichni potenciální zájemci (dodavatelé).

Za účast na předběžné tržní konzultaci nenáleží dodavatelům žádné kompenzace jejich případných nákladů. Předběžná tržní konzultace bude vedena tak, aby to nenarušilo hospodářskou soutěž, ani zásady zadávání veřejných zakázek ve smyslu § 6 ZZVZ.



Předběžné tržní konzultace budou probíhat takto:

- a) **Do 25. 04. 2025 do 12:00 hodin písemně** – dodavatelé prostřednictvím profilu zadavatele vyjádří svůj zájem zúčastnit se PTK a prostřednictvím E-ZAK zašlou PMDP představení své společnosti/subjektu a **Návrh řešení/nabídku služeb v oblasti MFA, které nabízejí**.
- b) PMDP osloví zájemce, jejichž návrh řešení odpovídá požadavkům PMDP, a s těmito povede osobní jednání; s každým zájemcem o zakázku bude jednáno samostatně a termín jednání bude dohodnut individuálně, vždy na základě písemné výzvy PMDP. Pokud více zájemců nabídne shodné řešení MFA od jednoho výrobce, je na rozhodnutí PMDP, se kterým zájemcem povede osobní jednání. Ke každému nabízenému typu MFA řešení bude vedeno vždy pouze jedno osobní jednání zaměřené na technické detaily řešení, neboť účelem osobního jednání je získat informace o produktu (výrobci) a ne o zájemci (dodavateli). Jednání budou probíhat v sídle PMDP na adrese Denisovo nábřeží 12, Plzeň.
- c) Cílem jednací fáze je především seznámit se se zamýšleným/možným řešením potřeb a požadavků PMDP, definovat a konkretizovat případné zadávací podmínky a hodnotící kritéria pro výběr dodavatele a získat nezávazné indikativní nabídky.
- d) Ukončení PTK PMDP předpokládá **nejpozději do 20. 06. 2025**.

Veškerá jednání v rámci PTK budou vedena pouze v českém jazyce, případně ve slovenském jazyce. Všechny shora uvedené způsoby vedení PTK jsou představou PMDP v době, kdy je tato PTK zahajována. PMDP nevylučuje, a v této souvislosti si vyhrazuje právo, že bude vést jednání v rámci PTK i jinými způsoby než shora uvedenými, vždy však za dodržení zásad uvedených v § 6 ZZVZ.

Případné upřesňující či doplňující dotazy, které musí být ve strojově čitelné formě, mohou dodavatelé zasílat prostřednictvím elektronického nástroje E-ZAK (viz odkaz výše). Odpovědi PMDP na případné upřesňující či doplňující dotazy ze strany dodavatelů budou v průběhu předběžných tržních konzultací zveřejňovány na profilu zadavatele. Na otázky, na které by odpovědi dle zadavatele obsahovali citlivé informace, nebude odpovězeno (resp. odpověď nebude tyto citlivé informace obsahovat).

Kontaktní osoba PMDP v těchto PTK:

Martin Stupka, stupka@pmdp.cz

Vyplyne-li z těchto předběžných tržních konzultací potřeba provedení dalších konzultací s dodavateli, oznámí PMDP další kolo předběžných konzultací způsobem, jakým byly oznámeny tyto předběžné tržní konzultace.

Pokud budou mít informace získané v průběhu předběžných tržních konzultací vliv na zadávací dokumentaci zakázky, budou tyto informace uvedeny v samostatné zprávě, která bude součástí zadávací dokumentace.

4. OBECNÝ ZÁMĚR A PŘEDSTAVA PMDP

Obecným záměrem PMDP je získání informací k možnostem implementace a provozu systému MFA.

Předmět a doba plnění budoucí veřejné zakázky

Předmětem plnění budoucí veřejné zakázky by mělo být implementace systému MFA v PMDP, zakoupení licencí resp. předplatného a technické podpory nejméně na období 3 let.



Bližší specifikaci předmětu plnění veřejné zakázky, resp. konkrétní možnosti a ideální návrh doby trvání plnění (na jak dlouhou dobu uzavřít smlouvu s vybraným dodavatelem), by PMDP rádo získalo na základě návrhu jednotlivých dodavatelů v rámci těchto PTK, spolu s příslušným odůvodněním.

5. VÝZVA PMDP K VYJÁDŘENÍ ZÁJMU O ZAKÁZKU A NÁVRH ŘEŠENÍ

PMDP tímto vyzývá potenciální dodavatele k účasti na těchto PTK a zaslání návrhu řešení, o němž bude jednáno v rámci vedení těchto PTK (v tomto dokumentu rovněž jako „Návrh řešení“).

Účastníci jsou pro účely jednání s PMDP v jednací fázi těchto PTK povinni zpracovat základní Návrh řešení dle technického zadání v Příloze č. 1, přičemž základní struktura Návrhu řešení může být (ale nemusí) následující:

- a) představení účastníka a všech jeho uvažovaných poddodavatelů;
- b) reference relevantní k nabízenému řešení;
- c) kontaktní adresu, telefonický kontakt a e-mailovou adresu pro komunikaci mezi zájemcem a PMDP;
- d) popis nabízeného systému MFA, jeho vlastnosti, moduly, základní principy fungování, způsob administrace, způsob a postup řešení bezpečnostních incidentů v rámci systému;
- e) varianty nabízeného systému MFA a jejich porovnání;
- f) orientační cena licencí/předplatného/technické podpory nabízeného systému MFA podle variant (bez ceny za implementaci);
- g) odhady doby potřebné pro nasazení systému MFA v PMDP (počty uživatelů a koncových bodů jsou uvedeny v Příloze č.1).
- h) praktická ukázka systému,
- i) představení možných scénářů (např. uživatel má PC/NB + smartphone, uživatel má PC/NB + tlačítkový telefon, uživatel má PC/NB bez čtečky karty + smartphone, apod.).

Návrh řešení může obsahovat jakékoliv další údaje dle uvážení zájemce o spolupráci.

Návrh řešení bude ze strany PMDP využit výlučně pro účely přípravy na jednání se zájemcem o zakázku, příp. pro účely zpracování finální zadávací dokumentace veřejné zakázky.

PMDP tímto prohlašuje, že v rámci vedení předběžných tržních konzultací bude respektovat práva dodavatele, co se týče ochrany obchodního tajemství a důvěrných informací poskytovaných účastníky předběžných tržních konzultací, budou-li tyto informace jako důvěrné dodavatelem označeny.

Pokud následně zadávací dokumentace bude obsahovat informace, které jsou výsledkem této předběžné tržní konzultace, PMDP označí v zadávací dokumentaci tyto informace, identifikuje osoby, které se na předběžné tržní konzultaci podílely, a uvede všechny podstatné informace, které byly obsahem předběžné tržní konzultace.

Plzeňské městské dopravní podniky, a.s.

Mgr. Jan Schejbal, MBA

vedoucí odboru Příjmy z dopravy



Příloha č. 1 - Technické zadání pro předběžnou tržní konzultaci: systém vícefaktorového ověřování uživatelů (MFA)**1. Požadavky na systém*****Funkční požadavky***

Systém je zamýšlen pro ověřování převážně koncových uživatelů, nejedná se tedy o systém typu Privileged Access Management (PAM). Systém ale musí být použitelný i pro vícefaktorové ověření účtů s vyšším oprávněním (vícefaktorové přihlášení k virtuálním serverům, které nemají fyzický USB port).

Je požadován systém umožňující vícefaktorové ověřování do On-premise Active Directory domény (z koncových stanic a vybraných HW i virtuálních serverů, vše s OS Windows), VPN, RDP a vybraných webových aplikací, publikovaných do prostředí internetu (podporující ověřování přes SAML 2.0). Systém musí být schopen zajistit minimálně druhý faktor pro přihlášení do výše zmíněných aplikací (ke stávajícímu jménu a heslu). Řešení vícefaktorového ověřování je preferováno pomocí OTP (one time password), který je generovaný pomocí autentikátoru (aplikace v chytrém mobilním telefonu, HW token s displejem, případně náhradní řešení – SMS, email apod.), nebo na základě biometrie (ověření obličejem, otiskem prstu apod.). Řešení pomocí SmartCard nebo USB tokenů není preferováno, ale není zcela znemožněno. Vícefaktorové přihlášení ke koncové stanici musí být možné i v případě, že stanice není připojena k síti LAN nebo je připojena do LAN mimo doménu (off-line režim). Přidělování tokenů uživatelům a nastavení přístupu do aplikací musí být pro administrátory centralizované a přehledné, musí být možnost, jak uživateli doručit přidělený token vzdáleně (zasláním QR kódu, číselného kódu apod.). Musí být možnost, jak řešit přihlášení uživatele v případě ztráty / rozbití jeho autentizačního tokenu (HW token, mobilní telefon apod.) např. možností vygenerování emergency přihlašovacího kódu administrátorem, v krajním případě dočasně vypnout potřebu MFA ověření pro vybraného uživatele apod.

Dvoufaktorové ověřování je v PMDP aktuálně používáno k přístupu do LAN přes VPN, současný systém je uvažováno buď rozšířit nebo zaměnit za jiný, tak aby splňoval všechny požadavky. V PMDP je též využíván systém šifrování pevných disků koncových stanic (hlavně přenosných), navrhovaný systém MFA musí být se systémem šifrování disků kompatibilní nebo musí být navrženo nahrazení systému šifrování disků za produkt kompatibilní s navrhovaným MFA.

Systém MFA musí být připraven i na případný budoucí přechod On-premise AD domény do Microsoft 365 (ověřování v Azure AD) a musí podporovat MFA ověřování i do systémů Microsoft 365. O nutnosti MFA ověřování do jiných cloudových systémů (Amazon, Google apod.) zatím není v PMDP uvažováno, jejich podpora ze strany nabízeného MFA je přípustná.

Technické požadavky

Kompatibilita: Systém musí být kompatibilní s různými, aktuálně podporovanými verzemi operačního systému Windows (varianty Pro i Server), v budoucnu se může vyskytnout požadavek na nasazení na platformě OS Linux, a různými zařízeními (koncové stanice, servery, případně mobilní zařízení). Systém musí umožňovat využití MFA v rámci stávajícího VPN připojení do sítě LAN. Systém musí být kompatibilní s používaným systémem šifrování disků koncových stanic, nebo musí být v rámci návrhu implementace MFA navržen jiný, kompatibilní systém šifrování disků koncových stanic.



Škálovatelnost: Systém musí být škálovatelný a schopný pokrýt potřeby PMDP i pro případ případného budoucího rozšíření požadavků na funkčnost nebo na počet klientů a serverů.

Vysoká dostupnost: Systém musí být nasazen v režimu vysoké dostupnosti (minimálně Active-Pasive režim), kdy i v případě výpadku jednoho z ověřovacích serverů bude možné se do domény / zařízení / VPN / aplikace přihlásit a dvoufaktorově uživatele ověřit.

Integrace: Systém musí být schopen integrace s existujícími bezpečnostními nástroji a platformami, jako jsou SIEM (Security Information and Event Management) systémy, konkrétně zasílání logů do systému Logmanager (syslog).

Výkon: Systém musí mít minimální dopad na výkon koncových zařízení a síťovou infrastrukturu.

Bezpečnostní požadavky

Autentizace a autorizace: Systém sám pro svojí správu musí podporovat vícefaktorovou autentizaci a role-based access control (RBAC) pro správu přístupů.

Compliance: Systém musí splňovat relevantní bezpečnostní standardy a regulace (např. GDPR, ISO/IEC 27001, návrh NIS2 apod.).

Požadavky na licence

Počet koncových bodů: Přibližně 65 serverů s OS Windows, přibližně 350 koncových stanic (uživatelů) s OS Windows.

2. Požadavky na výrobce / dodavatele

Podpora a údržba: Výrobce / dodavatel systému musí poskytovat pravidelné aktualizace a podporu pro systém vícefaktorového ověřování.

Dokumentace: Výrobce musí poskytnout kompletní dokumentaci k systému, včetně uživatelských příruček a technických specifikací. Musí být zpracován Disaster Recovery plán, kdy dojde k hypotetickému zhroucení systému MFA ověřování (možnost rychlého návratu k ověřování pouze jménem a heslem).

Školení: Výrobce / dodavatel systému musí zajistit školení pro administrátory na implementovaný systém.

Reference: Dodavatel musí mít prokazatelné zkušenosti s implementací MFA systémů v organizacích podobné velikosti.

