SPRÁVA ŽELEZNIC

Váš dopis zn.
Ze dne
Naše zn. 40054/2023-SŽ-GŘ-O8
Listů/příloh 3/1

Vyřizuje Miriam Hemzová
Mobil
E-mail Hemzova@spravazeleznic.cz

Datum 12. 06. 2023

Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem „Nasazení MFA a pořízení nosičů certifikátů"

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen „*Zadavatel*") Vás touto cestou informuje o tom, že připravuje zadávací řízení na veřejnou zakázku „Nasazení MFA a pořízení nosičů certifikátů". Vyhlášení této veřejné zakázky bude předcházet předběžná tržní konzultace (dále jen „*PTK*"), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení a způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Hlavními cíli projektu Nasazení MFA a pořízení nosičů certifikátů jsou zejména:

- Zvýšení bezpečnosti ICT prostředí SŽ, ochrana před zneužitím uživatelských účtů a oprávnění.
- Zajištění vysoce bezpečné autentizace uživatelů vůči systému poskytujícímu autentizační služby v ICT prostředí SŽ.
- Zajištění systematické a strukturované správy prostředků bezpečné identifikace a autentizace uživatelů (uživatelských certifikátů, fyzických nosičů).
- Nastavení procesů pro správu celého životního cyklu uživatelských certifikátů a jejich nosičů, podpora těchto procesů odpovídajícím IT systémem s vysokou mírou automatizace a definovanou bezpečnostní segregací rolí při správě certifikátů a jejich nosičů.
- Splnění legislativních požadavků (ZoKB, VoKB[1]).
- Naplnění platných interních předpisů SŽ.

Součástí projektu bude i implementace procesů bezpečné autentizace uživatelů i při nedostupnosti nosiče certifikátu (alternativní způsoby autentizace, náhradní pracovní postupy apod.).

Předmětem PTK bude zejména diskuze o níže uvedených tématech. Výčet témat je pouze demonstrativní a může být Zadavatelem rozšířen nebo zúžen kdykoliv před konáním PTK nebo i v průběhu PTK samotné, vyplyne-li tato potřeba z průběhu PTK. Zájmem Zadavatele je získat, co nejkomplexnější a nejucelenější soubor informací, které jsou pro vyhlášení předmětné veřejné zakázky nezbytné a žádoucí.

[1] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZoKB);
Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (VoKB)

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Generální ředitelství
Dlážděná 1003/7
110 00 Praha 1

Okruh témat a dotazů:

1. **Specifikace předmětu plnění a nastavení jeho rozsahu, fází, dílčích kroků, nastavení parametrů poptávaných služeb.**
2. **Doba potřebná k realizaci předmětu plnění.**
3. **Předpokládaná hodnota veřejné zakázky, dostatečnost podkladů nezbytných pro stanovení nabídkové ceny (resp. nacenění).**
4. **Předběžné požadavky na systém správy životního cyklu uživatelských certifikátů.**
5. **Předběžné požadavky na vlastnosti nosičů certifikátů a systém správy jejich životního cyklu.**

PTK je podle Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. 2. 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES a podle § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „*Zákon*") možností zadavatele předtím, než vyhlásí veřejnou zakázku, přičemž zadavatel má možnost v rámci PTK komunikovat s dodavateli (případně dalšími relevantními osobami) s cílem připravit zadání veřejné zakázky a informovat hospodářské subjekty (resp. dodavatele) o svých plánech a požadavcích při zadávání veřejných zakázek – zadavatel přitom může v rámci PTK i zjišťovat možnosti dodavatelů a případně i jejich návrhy řešení.

V rámci PTK bude představen nejprve záměr Zadavatele, včetně některých navrhovaných detailů, které se týkají, jak předmětu veřejné zakázky, tak zadávacího řízení. Dodavatelé pak budou mít možnost se k navrhovaným parametrům veřejné zakázky vyjádřit. Tímto postupem dojde ke zvýšení transparentnosti zadávacího řízení a k získání relevantních a objektivních informací o možnostech trhu, tak aby mohl Zadavatel optimálně nastavit zadávací podmínky veřejné zakázky, resp. celkové řešení zadávacího řízení.

Forma PTK: písemná, případně ústní

Způsob konání PTK:

1. **Fáze**: Zadavatel v rámci této pozvánky a její přílohy obeznamuje potenciální účastníky PTK se svým záměrem a potřebami. Zadavatel touto PTK cílí zejména na potenciální dodavatele působící na relevantním trhu. Za tímto účelem Zadavatel předkládá jako přílohu této pozvánky, aktuální bližší specifikaci připravované veřejné zakázky. Dodavatelé, kteří po prostudování poskytnuté specifikace budou mít zájem o další účast na PTK, potvrdí Zadavateli svou účast na email a v termínu uvedeném níže. Zadavatel má zájem o co nejširší účast na PTK, a proto v případě, že dodavatel projeví svůj zájem opožděně, Zadavatel takového dodavatele zahrne do procesu PTK. To neplatí v případě, že to již nebude technicky možné či vzhledem k pokročilosti procesu PTK vhodné.
2. **Fáze**: Dodavatelům, kteří na základě pozvánky zveřejněné Zadavatelem potvrdí ve stanovené lhůtě svůj zájem o účast na PTK, budou ze strany Zadavatele zaslány dokumenty: specifikace předmětu plnění, informace k systémům SŽ, dotazy k nabízenému řešení, základní obchodní podmínky a Platforma 2.0. a to prostřednictvím e-mailu, na emailovou adresu kontaktní osoby dodavatele. Tuto osobu určí dodavatel a v rámci potvrzení své účasti sdělí její kontaktní údaje. Dotazy budou zaslány nejpozději do 10 dnů od ukončení registrace.
3. **Fáze**: Odpovědi, které obdrží Zadavatel od dodavatelů ve lhůtě, která bude dodavatelům sdělena společně s konkrétními dotazy, budou Zadavatelem pečlivě analyzovány a vyhodnoceny. S ohledem na účel PTK Zadavatel přihlédne i k opožděným odpovědím, bude-li to možné a vhodné pro účel PTK. Zadavatel však žádá účastníky, aby stanovené termíny dodrželi. Dojde-li Zadavatel k závěru, že některá témata zůstávají nadále nejasná, sporná či vyvstane potřeba objasnění dalších doplňujících dotazů, přistoupí Zadavatel ke konání dalšího kola PTK, které bude uskutečněno nejspíše opět písemnou

formou prostřednictvím e-mailu, Zadavatel si však vyhrazuje možnost požádat zástupce dodavatelů o realizaci prezenčního jednání. Tento postup bude Zadavatelem opakován, dokud nebudou obdrženy veškeré informace potřebné ke správnému nastavení parametrů veřejné zakázky s názvem „Nasazení MFA a pořízení nosičů certifikátů“ ". Zadavatel o dalším průběhu PTK osloví vždy minimálně ty dodavatele, kteří projevili zájem o PTK v předcházejícím kole.

Pro bližší informace ohledně PTK se lze obrátit na níže uvedený email:

cnitptk@spravazeleznic.cz

Zadavatel sděluje, že připravovaná veřejná zakázka je plánována k zadání jako nadlimitní sektorová veřejná zakázka.

Předpokládaný počátek plnění předmětu veřejné zakázky je 1. kvartál roku 2024. Předpokládaná délka trvání veřejné zakázky je 12 měsíců, přičemž tato délka může být na základě realizované PTK upravena.

V případě Vašeho zájmu o účast na této PTK potvrďte, prosím, Vaši účast na emailovou adresu: cnitptk@spravazeleznic.cz, **a to nejpozději do 21. 06. 2023.**

Dodavatel by ve výše uvedeném potvrzení měl uvést minimálně:

- **název dodavatele a sídlo dodavatele;**
- **IČO dodavatele;**
- **jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail).**

PTK nesmí vést k porušení základních zásad Zákona. Průběh i výsledek PTK proto bude zaznamenán ve zprávě vytvořené Zadavatelem. Informace z PTK užité v zadávacích podmínkách veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, a to včetně osob, které se na PTK podílely. Zadavatel současně uvede v zadávacích podmínkách i všechny podstatné informace, které byly obsahem PTK a ovlivnily nastavení zadávacích podmínek.

Děkuji za spolupráci.

S pozdravem

Ing. David Miklas
12.06.2023 16:03
Podepsáno elektronicky

Ing. David Miklas
ředitel Správy železniční telematiky

Přílohy:
Příloha č.1 – Specifikace předmětu plnění

Příloha 1 – Předběžná specifikace předmětu plnění

Předběžná tržní konzultace k připravované veřejné zakázce *„Nasazení MFA[1] a pořízení nosičů certifikátů"*

Správa železnic, státní organizace (dále jen *„SŽ"*) plánuje implementaci systému vysoce bezpečné vícefaktorové autentizace (MFA) založené na uživatelských certifikátech, systému pro správu životního cyklu uživatelských certifikátů a jejich fyzických nosičů. Cílem této předběžné tržní konzultace je získání relevantních informací o možných nebo vhodných řešeních pro případné zadání jedné nebo více budoucích veřejných zakázek dostatečně přesným, technologicky neutrálním a nediskriminujícím způsobem a současně postupem, který bude vyhovovat požadavkům a prostředí SŽ.

Záměr SŽ v oblasti MFA a pořízení nosičů certifikátů

Záměrem projektu je zavedení prostředků pro identifikaci uživatelů a jejich vysoce bezpečné ověření (autentizaci) při přístupu k ICT/IoT aktivům SŽ. Implementace systému vícefaktorové autentizace (MFA) s využitím uživatelských certifikátů vydaných důvěryhodnými interními certifikačními autoritami je v souladu s dlouhodobou koncepcí bezpečné identifikace a autentizace uživatelů a zvýšení zabezpečení přístupů k aktivům SŽ.

Autenticita uživatelů bude ověřována bezpečným systémem vůči autentizačním službám typu Identity Provider (v aktuálním prostředí SŽ: vůči systémům Microsoft Active Directory[2]). SŽ v rámci tohoto projektu plánuje zavedení systému autentizace uživatelů založeném na interních uživatelských certifikátech vystavených důvěryhodnými interní certifikačními autoritami a uložené na bezpečném fyzickém nosiči certifikátu. Současně je požadováno, aby fyzický nosič certifikátu byl certifikován jako kvalifikovaný prostředek pro elektronické podpisy založené na kvalifikovaném certifikátu[3]. Dalším požadavkem na fyzický nosič certifikátu je poskytování bezdrátových (bezkontaktní) identifikace, popř. ověření uživatele, zejména vůči systémům fyzické bezpečnosti (přístupové systémy) a dalším systémům využívající bezkontaktní identifikaci.

Cíl projektu „Nasazení MFA a pořízení nosiče certifikátů"

Hlavními cíli projektu Nasazení MFA a pořízení nosičů certifikátů jsou zejména:

- Zvýšení bezpečnosti ICT prostředí SŽ, ochrana před zneužitím uživatelských účtů a oprávnění.
- Zajištění vysoce bezpečné autentizace uživatelů vůči systému poskytující autentizační služby v ICT prostředí SŽ.
- Zajištění systematické a strukturované správy prostředků bezpečné identifikace a autentizace uživatelů (uživatelských certifikátů, fyzických nosičů).
- Nastavení procesů pro správu celého životního cyklu uživatelských certifikátů a jejich nosičů, podpora těchto procesů odpovídajícím IT systémem s vysokou mírou automatizace a definovanou bezpečnostní segregací rolí při správě certifikátů a jejich nosičů.

[1] MFA – vícefaktorová autentizace
[2] V prostředí UAS (uživatelsko-administrativní síť) i prostředí TDS (technické datové sítě)
[3] Certifikována jako QSCD (kvalifikovaný prostředek pro vytváření elektronických podpisů) podle eIDAS (Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES)

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384
Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz
Generální ředitelství
Dlážděná 1003/7
110 00 Praha 1

- Splnění legislativních požadavků (ZoKB, VoKB[4]).
- Naplnění platných interních předpisů SŽ.

Součástí projektu bude i implementace procesů bezpečné autentizace uživatelů i při nedostupnosti nosiče certifikátu (alternativní způsoby autentizace, náhradní pracovní postupy apod.).

Na pořizované nosiče certifikátů SŽ klade další požadavky, zejména:

- musí být kvalifikovaným prostředkem pro vytváření elektronického podpisu založeného na kvalifikovaném certifikátu kompatibilním se službami definované akreditované certifikační autority vydávající kvalifikované certifikáty[5];
- musí být osazeny bezdrátovou (bezkontaktní) částí kompatibilní se systémy fyzické bezpečnosti (přístupové systémy), popř. poskytující další definované služby (bude upřesněno v rámci konkrétních oblastí PTK);
- zajištění hardwarové a softwarové kompatibility se čtečkami nosičů certifikátů a obslužným SW pro hlavní OS (Windows, macOS) používaným v ICT prostředí SŽ
- možnost potisku nosiče definovanými optickými identifikačními údaji (vhodnou technologií tisku nebo polepu) s případnou mechanickou ochranou potisku a dalšími ochrannými prvky
- definovaná mechanická a elektronická odolnost nosičů certifikátů i jejich případného potisku.

Záměr projektu: předběžné požadavky předmět výběrového řízení, předpokládaný postup

Cílem výběrového řízení bude uzavření smlouvy, jejímž předmětem bude zejména:

- Poskytnutí služeb předimplementační analýzy, detailního návrhu řešení a prováděcího projektu,
- implementace a podpora systému pro správu životního cyklu uživatelských certifikátů vydávaných interními důvěryhodnými CA a umístěnými na nosiči certifikátů (pro prostředí UAS a TDS),
- integrace se službami Identity Provider (konkrétně ActiveDirectory) pro zajištění bezpečné identifikace a autentizace uživatelů s využitím uživatelských certifikátů (pro prostředí UAS a TDS),
- implementace a podpora klientského SW pro koncové stanice (pro zajištění bezpečné identifikace a autentizace uživatelů s využitím uživatelských certifikátů), včetně intuitivního výběru certifikátu pro příslušné prostředí (UAS, TDS[6]),
- dodávky fyzického nosiče certifikátu s definovanými technickými parametry, případně včetně služeb personalizace (potisku) fyzického nosiče,
- integrace systému správy uživatelských certifikátu se systémem vydávání kvalifikovaných certifikátů pro vytváření elektronického podpisu založeného na kvalifikovaném certifikátu,
- propojení (integrace) procesů vydávání fyzického nosiče certifikátu na systémy využívající nosič pro identifikaci uživatele pomocí bezdrátové technologie certifikátu (např. přístupové systémy fyzické bezpečnosti apod.),
- zajištění školení pracovníků Zadavatele na dodané technologie a konkrétní implementaci,
- služby na vyžádání.

SŽ předpokládá, že plnění bude realizováno v několika na sebe navazujících fázích:

Fáze 1: Před implementační analýza

Zpracování před implementační analýzy pro zavedení systému bezpečné identifikace a ověřování uživatelů, správy životního cyklu osobních uživatelských certifikátů, správy životního

[4] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZoKB);
Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (VoKB)
[5] V souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
[6] UAS – Uživatelsko-administrativní síť
TDS – Technologické datové sítě

cyklu nosičů certifikátů, způsobu napojení na související systémy a nastavení obslužných procesů a procesů obnovy.

Fáze 2: Implementace systému správy životního cyklu uživatelských certifikátů (pro UAS i TDS) a správy životního cyklu nosičů certifikátů

Implementace systému správy životního cyklu uživatelských certifikátů pro prostředí UAS i TDS, včetně systému personalizace nosičů.

Fáze 3: Implementace MFA s využitím uživatelských certifikátů (pro UAS i TDS)

Implementace vysoce bezpečné autentizace uživatelů vůči systému poskytující autentizační služby (konkrétně Active Directory) založené na uživatelských certifikátech, a to jak v prostředí UAS, tak v prostředí TDS.

Fáze 4: Napojení systému správy životního cyklu nosiče certifikátů na další definované systémy Zadavatele

Zajištění procesního, datového nebo aplikačního propojení systému správy životního cyklu uživatelských certifikátů a systému správy životního cyklu nosičů certifikátů s dalšími definovanými systémy.

Zejména bude požadována:

- integrace systému správy uživatelských certifikátu se systémem vydávání kvalifikovaných certifikátů pro vytváření kvalifikovaného elektronického podpisu
- propojení (integrace) procesů vydávání fyzického nosiče certifikátu se systémy využívající nosič pro identifikaci uživatele (především pomocí bezdrátové technologie, např. přístupové systémy fyzické bezpečnosti)

Fáze 5: Akceptační, výkonové a bezpečnostní testy, ověřovací (pilotní provoz), dokumentace řešení, školení

Po provedení implementace řešení provede dodavatel v souladu s metodikami definovanými v rámci před implementační analýzy akceptační funkční, výkonové a zátěžové testy a odstraní případné neshody.

Fáze 6: Zajištění přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů

Na základě návrhu procesu a harmonogramu přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů, definovaného v před implementační analýze, zajistí dodavatel potřebnou součinnost při realizaci tohoto přechodu.

Fáze 7: Průběžná dodávka nosičů certifikátů a jejich personalizace

Pro pilotní provoz (Fáze 5) a zajištění přechodu k novému řešení (Fáze 6) dodavatel průběžně zajistí dodávku příslušného množství nosičů certifikátů. Dále dodavatel zajistí dodávku nosičů certifikátů na základě dílčích objednávek Zadavatele.

Fáze 8: Technická podpora řešení

Pro implementované řešení poskytne dodavatel službu technické podpory implementovaného řešení.

Fáze 9: Služby na vyžádání

Dodavatel poskytne zadavateli služby konzultace na vyžádání. Služby mohou být čerpány především pro rozšiřování a rozvoj systému správy životního cyklu uživatelských certifikátů.

Konkrétní oblasti a otázky, které jsou předmětem předběžné tržní konzultace

Konkrétní oblasti a otázky, stejně tak i předběžné požadavky na funkční a nefunkční vlastnosti systému správy životního cyklu uživatelských certifikátů a předběžné požadavky na vlastnosti nosičů certifikátů budou zaslány pouze registrovaným účastníkům předběžné tržní konzultace, a to jako soubor informací a otázek k získání relevantních informací o vhodných řešeních pro splnění cílů projektu. Současně SŽ od předběžné tržní konzultace očekává, že získá od účastníků informace o možných přístupech k řešení, odhadovaných časových i finančních parametrech projektu.

SŽ poskytne registrovaným dodavatelům dokument s dotazy zejména v následujících oblastech:

- Oblast návrhu průběhu projektu.
- Předběžné vymezení a rozsahu projektu.
- Předběžné rozdělení projektu na navazující fáze.
- Předběžné požadavky na systém správy životního cyklu uživatelských certifikátů.
- Předběžné požadavky na vlastnosti nosičů certifikátů a systém správy jejich životního cyklu.