ČESKOMORAVSKÁ ZÁRUČNÍ A ROZVOJOVÁ BANKA, a.s.

Odesílatel:
Ústředí
Jeruzalémská 964/4
110 00 Praha 1

Váš dopis značky/ze dne	Naše značka	Vyřizuje/telefon	E-mail	Místo/datum
		[redacted]	[redacted]	Praha 6.10.2020

Výzva k předložení nabídky

Vážení,

Českomoravská záruční a rozvojová banka, a.s. (dále jen „banka“) jako veřejný zadavatel si tímto dovoluje oslovit Vaši společnost a vyzvat Vás k podání nabídky do výběrového řízení na veřejnou zakázku malého rozsahu, která je realizována mimo režim zadávacího řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Předmětem veřejné zakázky je penetrační test internetového bankovnictví, jehož součástí je i jednoduchá aplikace Komunikace s klienty. V rámci penetračního testu požadujeme i provedení přezkumu bezpečnostních opatření (metod) (dále jen „Přezkum“), který je povinný pro všechny poskytovatele platebních služeb (dle regulačních technických standardů RTS SCA, klíčové součásti Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015, o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (PSD2) (dále jen „Směrnice“).

Penetrační test bude proveden s tzv. znalostí. Dodavateli budou předány přihlašovací údaje do aplikace internetového bankovnictví. Podmínkou je mít telefon pro příjem autorizačních SMS, e-mailovou adresu a komerční certifikát od některého z kvalifikovaných poskytovatelů služeb vytvářejících důvěru (I.CA a.s., Česká pošta, s.p, eIdentity, a.s.). Tyto přihlašovací údaje umožňují i práci v režimu naplnění směrnice PSD2 a přístupu k účtu pomocí třetí strany. Dodavateli bude po uzavření smlouvy předána uživatelská dokumentace, detailně popisují postupy a práci v aplikaci internetového bankovnictví, tak i metody napojení na API PSD2 internetového bankovnictví. Součástí předané dokumentace bude i způsob práce v aplikaci Komunikace s klienty. Tvorba testovacích scénářů musí být součástí dodávky a zajistí jí dodavatel.

Přezkum by měl zahrnovat všechny povinné aspekty dle čl. 3 Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace (dále jen „Nařízení“).

Pro Vaši informaci Vám sdělujeme, že:
- banka nevyužívá výjimku dle čl. 18 Nařízení;
- banka uplatňuje silné ověření klienta s využitím dvou metod:
    a) certifikátu + silného hesla
    b) jednoznačného identifikátoru + silného hesla + autentizační SMS.
- API poskytuje funkce v rozsahu rolí daných směrnicí EU pro:
    a) Poskytovatele služeb nepřímého zadání platebního příkazu (PISP)
    b) Poskytovatele služeb informování o platebním účtu (AISP)
    c) Poskytovatele služeb platby platební kartou (PIISP, CISP)

- Internetové bankovnictví poskytuje API pomocí technologie webových služeb REST API. API je implementováno na základě standardu COBS České bankovní asociace, vytvořeného na základě směrnice EU PSD2, dle specifikace v 3.1
- V rámci API PSD2 jsou implementovány tyto služby:
    a) Metody pro všechny poskytovatele služeb
        - Registrace aplikace klienta
        - Informace o existující registraci aplikace
        - Změna existující registrace aplikace
        - Smazání existující registrace aplikace
        - Obnovení sdíleného tajemství client_secret
        - Obnovení aplikačního klíče API_KEY
    b) Metody pro poskytovatele služby informování o platebním účtu (AISP)
        - Seznam účtů
        - Zůstatek na účtu
        - Přehled transakcí
        - Dotaz na Dostatek prostředků
    c) Metody pro poskytovatele služby platby kartou (PIISP, CISP)
        - Dotaz na Dostatek prostředků
    d) Metody pro poskytovatele služby nepřímého zadání platebního příkazu (PISP)
        - Dotaz na Dostatek prostředků
        - Nová platba
        - Status platby
        - Detail platby (info)
        - Smazání neautorizované platby
        - Start Generování autorizační ID
        - Detail autorizace platby
        - Iniciace Autorizace platby
        - Finalizace Autorizace platby
        - Seznam autorizací plateb
        - Hromadné platby
        - Trvalé platby

V rámci plnění zakázky banka předpokládá provedení Přezkumu v:
1) aplikaci internetového bankovnictví, která je dostupná malé části klientů banky;
2) interní aplikaci následného zpracování zadaných plateb klienty, která je dostupná vybrané skupině zaměstnanců banky;
3) posouzení interních bezpečnostních pravidel a postupů při zpracování plateb pomocí uvedených aplikací.

Aplikace internetového bankovnictví a Komunikace s klienty jsou naprogramovány v prostředí Microsoft .NET, využívají COM objekty, softwarově orientovanou architekturu, bezpečné komunikační protokoly HTTPS a TLS, autentizační certifikáty a autentizační a autorizační SMS. V aplikacích jsou ve formulářích taktéž zabudovány kontroly vstupních dat.

Banka požaduje, aby v rámci:
- penetračního testu internetového bankovnictví bylo provedeno prověření možnosti prolomení bezpečnostních opatření jak ve webovém rozhraní, tak v API PSD2 a to takovým způsobem, který bude v rozporu s dodanou dokumentací (dodavatel nebude mít přístup do interního rozhraní aplikace internetového bankovnictví);
- penetračního testu aplikace Komunikace s klienty bylo provedeno prověření možnosti prolomení bezpečnostních opatření ve webovém rozhraní pro vyzvedávání zaslaných zásilek (dodavatel nebude mít přístup do interního rozhraní této aplikace);
- Přezkumu bylo provedeno posouzení bankou předložených materiálů a byla provedena diskuze pracovníků dodavatele s odbornými pracovníky banky z útvarů, jež mají danou problematiku ve své gesci; osoby provádějící Přezkum, musí mít odborné znalosti v oblasti bezpečnosti informačních technologií a plateb ve smyslu výše citovaného Nařízení; zpracovaný Přezkum bezpečnostních opatření musí být v samostatné příloze závěrečné zprávy Penetračního testu.

Místo a termín plnění zakázky – Českomoravská záruční a rozvojová banka, a.s., Na Florenci 5, Praha 1, ev. Jeruzalémská 4, Praha 1. Očekávané plnění zakázky je v období 4. čtvrtletí t. r.

Nabídka musí obsahovat:

- nabídku termínů provedení penetračního testu a Přezkumu – přesný termín bude dohodnut v rámci plnění zakázky,
- cenu za dodávku veřejné zakázky,
- jména osob, která se budou podílet na penetračním testování a Přezkumu, včetně doložení jejich odbornosti a certifikace,
- výslovný závazek dodavatele, že v případě náhrady osob provádějících penetrační testování a Přezkum v průběhu plnění zakázky, budou nové osoby splňovat odbornost minimálně na stejné úrovni jako osoby uvedené v nabídce; v případě, že zakázka nebude plněna osobami uvedenými v nabídce, případně místo nich osobami se stejnou či vyšší odborností, má banka právo odstoupit od smlouvy s účinky ex tunc.

Kritériem pro výběr dodavatele bude nejnižší celková (paušální) výše ceny za poskytnuté služby, přičemž dodavatel stanoví tuto cenu celou částkou za celý předmět plnění veřejné zakázky, a to v Kč bez DPH. Tato cena bude zahrnovat veškeré nutné vedlejší náklady dodavatele (např. cestovné, ubytování, komunikační a administrativní náklady).

Pokud Vás naše výzva zaujala, zašlete laskavě svou nabídku nejpozději do 16. 10. 2020, do 10:00 hod, na e-mail podatelna@cmzrb.cz, v předmětu e-mailu uveďte **„Nabídka do výběrového řízení na penetrační test internetového bankovnictví“**.

Banka si může v případě nejasností údajů uvedených v nabídce vyžádat od dodavatele písemné objasnění předložených informací či dokladů nebo předložení dalších informací či dokladů.

Dodavatel nemá právo na náhradu nákladů spojených s účastí ve výběrovém řízení. Dodavateli podáním nabídky nevznikají žádná práva na uzavření smlouvy.

Banka je oprávněna toto výběrové řízení zrušit kdykoliv bez udání důvodu. V případě zrušení výběrového řízení či neuzavření smlouvy s dodavatelem nenese banka jakoukoli odpovědnost za škodu z důvodu předsmluvního jednání ani žádnou odpovědnost za jakoukoli jinou újmu vzniklou v této souvislosti. Tímto se vylučuje aplikace veškerých ustanovení zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**OZ**“), týkajících se předsmluvní odpovědnosti, zejména ustanovení § 1728 až 1730 OZ.

Nabídka dodavatele je návrhem na uzavření smlouvy. Smlouva s vybraným dodavatelem bude uzavřena formou akceptování nabídky dodavatele ze strany banky, ledaže by se banka a dodavatel dohodli na jiné formě uzavření smlouvy.

Vzhledem k tomu, že banka má povinnost uveřejňovat své smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění, upozorňujeme potenciální dodavatele, že v případě, že hodnota předmětu plnění smlouvy (tj. nabídky a její akceptace), bude vyšší než 50.000,- Kč bez DPH, bude smlouva uveřejněna v registru smluv. Smlouva v takovém případě v souladu se zákonem o registru smluv nabude účinnosti dnem uveřejnění. Uveřejnění zabezpečí banka. Pokud nabídka bude obsahovat informace, které se nemají uveřejňovat v registru smluv, jelikož je dodavatel považuje za své obchodní tajemství nebo jde o údaje, které nepodléhají uveřejnění podle zákonů upravujících svobodný přístup k informacím, buďte tak laskavi a označte tyto informace v nabídce, a to včetně důvodu, proč nemají být uveřejněny.

S pozdravem

[redacted]
Manažer informační bezpečnosti