

115 03 PRAHA 1

Sekce správní
odbor obchodní

V Praze 30. července 2019
Č.j.: 2019/084214/CNB/420

Vysvětlení č. 1 zadávací dokumentace veřejné zakázky „Aplikační rozhraní pro třetí strany pro elektronický přístup k účtům klientů ČNB a předání platebních příkazů bance klienta dle směrnice PSD 2“

Zadavatel v souladu s § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „zákon“), v platném znění, níže poskytuje vysvětlení zadávací dokumentace výše uvedené veřejné zakázky, a to na základě žádosti dodavatele o vysvětlení.

Odkaz

Příloha č. 1 Kapitola 1. Obecné funkční požadavky na API Odstavec 1 a)

Otázka:

„V textu je pravděpodobně překlep. ČOBS v 3.0 je platný od 1.1 2020.“

Odpověď zadavatele:

Ano, jedná se o překlep. Veškerá API budou založena na standardu ČOBS min. verze 2.0 platné od 1.1.2019.

Příloha č. 1 Kapitola 1. Obecné funkční požadavky na API Odstavec 1 g)

„Zde dle textu je očekáván návrh integrace se systémy ČNB, odstavec je však kromě nadpisu prázdný. Můžete prosím upřesnit zda se nejedná o chybu?“

Odpověď zadavatele:

Ne, o chybu se nejedná. Návrh integrace se systémy ČNB vypracuje dodavatel v souladu s návrhem smlouvy.

Příloha č. 1 Kapitola 2. Povinné funkční požadavky na API

„Prosím o potvrzení, že součástí zadání dle funkčních požadavků nejsou: - hromadné platby - trvalé platby - instantní platby - multipodpisy - integrace s JERRS nebo PRETA.“

Odpověď zadavatele:

Zadavatel toto potvrzuje. Veškeré funkční

požadavky jsou definované v návrhu smlouvy a dle Českého standardu pro Opening Banking vydaný ČBA.

Příloha č. 1 Kapitola 2. Povinné funkční požadavky na API

„V textu se objevují zkratky ABO a ABO-K. Je náš výklad správný, když ABO je označení pro coresystem a ABO-K je rozhraní ke coresystemu? Je možné získat jako podklad veřejné zakázky wsdl nebo základní popis rozhraní ABO-K?“

Odpověď zadavatele:

Ano, váš výklad je správný. WDSL pro ABOK-WS je veřejně dostupný na <https://abok.cnb.cz/>.

Příloha č. 1 Kapitola 2. Povinné funkční požadavky na API

„Prosíme o upřesnění zda součástí požadavků na řešení jsou též: - generování reportů IPSIFE10 a IPSIFE20 resp. sběr podkladů pro reporty - implementace náhradního řešení k PSD2 vyhrazenému kanálu nebo žádost o výjimku - reporty výkonnosti a dostupnosti řešení - zátěžové testování - GUI pro revokace souhlasů uživatele.“

Odpověď zadavatele:

Ne, nejsou. Veškeré funkční požadavky jsou definované v návrhu smlouvy.

Příloha č. 1 Kapitola 1. Obecné funkční požadavky na API Odstavec 1 a)

„Můžete upřesnit zda je povolená odchylka od implementace COBS 3.0 spočívající v přesunu generování clientId a clientSecret a registrace redirectURL z API na developer portálu?“

Odpověď zadavatele:

Ne, není. Dodavatel musí provést implementaci v souladu s návrhem smlouvy.

Příloha č. 1 Kapitola 2. Povinné funkční požadavky na API Požadavek A-1

„Dle požadavku na implementaci COBS, předpokládáme správně, že plánujete implementaci autentizace TPP na základě PSD2 QCWeb certifikátu resp. mTLS?“

Odpověď zadavatele:

Ano, dodavatel to chápe správně.

Příloha č. 1 Kapitola 2. Povinné funkční požadavky na API Požadavek A-11

„Můžeme požádat o předání informací týkajících se způsobu autentizace koncového uživatele pomocí certifikátu? mTLS? Proti jakému internímu systému bude certifikát resp. informace

z certifikátu porovnáváno resp. s jakým systémem máme předpokládat integraci? “.

Odpověď zadavatele:

Autentizace bude pomocí certifikátu, nebo pomocí jména, hesla a autentizační sms, a to proti ABOK.

Příloha č. 1 Kapitola 3. Specifické požadavky na API Požadavek B-1

„V současné chvíli nejsou známy všechny možné certifikační autority, které mohou vydávat PSD2 QCWeb certifiáty, stejně tak jasné, zda se všechny autority budou řídit ETSI ve stejné verzi. Navrhujeme omezení na ETSI 1.1.1 a ETSI 1.3.1 řešit nejprve pouze pro ICA. Autentizaci TPP certifikáty PSD2 QCSeal předpokládáme, že nebudete řešit. “.

Odpověď zadavatele:

Zadavatel trvá na znění požadavku B-1.

Příloha č. 1 Kapitola 3. Specifické požadavky na API Požadavek B-2

„Zde nerozumíme požadavku, prosíme o upřesnění. Chcete zabezpečit přenášená data v požadavku elektronickým podpisem koncového uživatele? API volá aplikace TPP, která nebude mít jednoduchou a bezpečnou možnost zajistit podepsání požadavku koncovým uživatelem. “.

Odpověď zadavatele:

Ano, tento požadavek vyplývá přímo ze znění požadavku B-2.

Příloha č. 1 Kapitola 3. Specifické požadavky na API Požadavek B-4

„Jakou reálnou dostupnost prosím požadujete? Požadavkem na 7x24 rozumíme, že instalace a konfigurace bude provedena tak, aby bylo možné provádět servisní a administrační práce bez nutnosti odstávky. “.

Odpověď zadavatele:

Ano, požadujeme 7x24. Zadavatel tedy požaduje dostupnost bez nutnosti odstávky.

Příloha č. 1 Kapitola 3. Specifické požadavky na API Požadavek B-6

„Jde o celkovou dobu odezvy včetně volání ABO-K resp. BE? Pokud ano, jakou maximální latenci požadujete po dodávaném řešení? “.

Odpověď zadavatele:

1 vteřina, viz. požadavek B-6.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ002

„Předpokládáme správně, že požadujete zavedení CICD resp. nástroj pro automatický nasazení dodávky do zvoleného prostředí? Používáte pro CICD již nějaký nástroj např. GITLAB pipeline nebo Jenkins?“.

Odpověď zadavatele:

Ano, pro přenos kódu z testovacího do produkčního prostředí je použit formální proces obsahující schvalování odpovědnou osobou zadavatele. Nástroje GITLAB pipeline ani Jenkins nepoužíváme.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ006

„Týká se zmíněné omezení na nemožnost VPN vzdáleného přístupu pracovníky podpory i neprodukčních prostředí?“.

Odpověď zadavatele:

Přístup ke všem prostředím provozovaným ve vnitřní síti ČNB není pro dodavatele možný vzdáleně.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ009

„Má ČNB již systém pro centrální logování např. ELK? Nebo je možné použít SIEM? Je možné použít ELK včetně bezpečnostního rozšíření zajišťující autentizaci a autorizaci správců?“.

Odpověď zadavatele:

ELK nepoužíváme, lze použít SIEM ArcSight.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ013

„Předpokládá tímto požadavkem (přesun dat mimo prostředí pouze po anonymizaci) objednatel nějakou implementaci na straně dodavatele?“.

Odpověď zadavatele:

Ne.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ014

„Předpokládáme, že požadavek na archivaci se netýká všech dat. Pro vyjasnění našeho pohledu uvedu výčet. Příklad archivovatelných dat: - auditní, statistické a provozní logy - podklady pro reporty - souhlasy koncových uživatelů s přístupem TPP Příklad nearchivovatelných dat: - clientId, clientSecret, název aplikace TPP - access a refresh token.“.

Odpověď zadavatele:

Trváme na původním znění BEZ014. Zadavatel požaduje archivovat úplně všechna data.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ016

„Jde o metodický list pro bezpečný vývoj dodavatele? Nebo jej stanoví objednatel? V případě, že jej stanoví objednatel, můžeme o něj požádat?“.

Odpověď zadavatele:

Vývoj SW je prováděn dle principů secure-SDLC, viz metodický list, který tvoří přílohu č. 3 návrhu smlouvy.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ017

„Toto lze zajistit jen u kódu, na který se vztahují autorská práva dodavatele resp. týká se to pouze Modifikací. Části naší dodávky by byly komponenty a programové vybavení třetích stran pod Apache 2.0 licencí. Je to pro ČNB akceptovatelné?“.

Odpověď zadavatele:

Úprava autorských práv je vymezena v návrhu smlouvy, zejména v čl. VII návrhu smlouvy. Zadavatel v této fázi nemůže předjímat to, zda dodavatelem specifikované plnění je v souladu s podmínkami účasti. Tato otázka bude posuzována až po uplynutí lhůty pro podání nabídek.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ018

„Jde o metodický list pro kryptografie stanovený dodavatelem? Nebo jej stanoví objednatel? V případě, že jej stanoví objednatel, můžeme o něj požádat?“.

Odpověď zadavatele:

Ano, Metodické listy lze předat dodavateli na základě jeho předchozí žádosti v souladu s čl. 9.4 Zadávací dokumentace.

Příloha č. 1 Kapitola 4. Bezpečnostní požadavky
Požadavek BEZ024

„Máte seznam vámi povolených algoritmů. Naše řešení ukládá pouze saltované hashe pomocí SHA256.“.

Odpověď zadavatele:

Požadavek se týká tvorby tokenů/autorizačních kódů – při jejich generování musí být použit algoritmus v současné době považovaný za dostatečně bezpečný. Tokeny zejména nesmí být

uhodnutelné, nebo odvoditelné, viz metodický list, který tvoří přílohu č. 3 návrhu smlouvy.

Článek III Testování, předání a převzetí díla
Odstavec 6

„Považujete i dva roky starou knihovnu jquery za bezpečnostní riziko kategorie A?“.

Odpověď zadavatele:

Všechny zranitelnosti zjištěné Penetračním testem jsou vždy kategorie A, viz. čl III, odst. 6 návrhu smlouvy.

Příloha č. 1 ZD Návrh smlouvy, II. 1 a)

„Průměrná délka realizací dodávky celého PSD2 řešení do 3 bankovních domů v Čechách, které máme úspěšně za sebou, byla 8 měsíců, jen analýza trvala 1-2 měsíce. Víme také, že jiné projekty trvaly přes 2 roky. Termín 2 měsíce na technickou dodávku je z naší zkušenosti nereálný. Je možné nastavit harmonogram realizace dle parametrů vítězné dodávky. Je možné případně návrh smlouvy takto upravit?“.

Odpověď zadavatele:

Zadavatel trvá na současném znění termínů stanovených v návrhu smlouvy.

Příloha č. 1 ZD Návrh smlouvy, IV. 2 d)

„V rámci podpory je požadavek na nestálý soulad se všemi předpisy. Toto však není možné paušálně nacenit, neboť netušíme, jaké změny mohou být požadovány. Samozřejmě budeme řešení udržovat v souladu, avšak na základě placených změnových požadavků, odsouhlasených Zadavatelem. Je možné takto smlouvu upravit?“.

Odpověď zadavatele:

Zadavatel trvá na současném znění.

Příloha č. 1 ZD Návrh smlouvy, IV. 2 e)

„Pokud je aktualizace (např. nová verze SW) uvolněna do produkce, musí následně proběhnout upgrade u Zadavatele v testovacím prostředí a následně na produkci, což může být i projektová dodávka. Není možné jej tedy v ten samý den nasadit. Počet a náročnost upgradů není možné definovat, proto navrhuje, že by aktualizace byla realizována na základě placených změnových požadavků, odsouhlasených Zadavatelem. Je možné takto smlouvu upravit?“.

Odpověď zadavatele:

Zadavatel trvá na současném znění.

Příloha č. 1 ZD Návrh smlouvy, IV. 2 e)

„V uvedeném bodě nám chybí specifikace programového vybavení o které se jedná, resp. odkaz na programové vybavení, které je součástí dodávky v rámci této smlouvy. Je možné tuto specifikaci doplnit?“.

Odpověď zadavatele:

Programové vybavení je specifikováno v rámci čl. I odst. 1 návrhu smlouvy.

Příloha č. 1 ZD Návrh smlouvy, IV. 2 c)

„Prosíme o potvrzení zda se jedná o podporu v režimu 5x8 (jak je uvedeno v článku IV.2 b). Uvedené časy (24 hodin) jsou hodiny pracovní?“.

Odpověď zadavatele:

Podpora dle čl. IV odst. 2 písm. c) návrhu smlouvy předpokládá, že vady programového vybavení závažnosti 1 musí být odstraněny do 24 hodin od oznámení jejich vady a vady závažnosti 2 do 48 hodin od jejich oznámení, tyto lhůty přitom běží i mimo pracovní dny. Vady závažnosti 3 mají být odstraněny do 5 pracovních dnů od jejich oznámení. Režim „5x8“ se však vztahuje na služby podpory při řešení provozních problémů přímo souvisejících s programovým vybavením ve formě konzultací upravené v rámci čl. IV odst. 2 písm. b) návrhu smlouvy.

Příloha č. 1 ZD Návrh smlouvy, VII.

„Zadavatel požaduje právo zasáhnout do zdrojových kódů. To samozřejmě je v pořádku, avšak tím, že případné chyby vzniklé úpravou není možné odstraňovat v rámci paušální ceny podpory, na náklady poskytovatele a ve lhůtách stanovených pro opravu chyb poskytovatele. Je možné takto smlouvu upravit?“.

Odpověď zadavatele:

Zadavatel trvá na současném znění.

Příloha č. 1 ZD Návrh smlouvy, III. 6.

„Prosíme o informaci, zda je možné získat přesnou detailní specifikaci penetračních testů a to včetně metodiky hodnocení kritičnosti jednotlivých nálezů. Nedomníváme se, že je možné všechny potenciální nálezy, zvláště zcela minoritní, považovat za chybu A. Je možné takto smlouvu upravit?“.

Odpověď zadavatele:

Veškeré relevantní informace jsou obsažené v návrhu smlouvy.

Příloha č. 1 ZD Návrh smlouvy, III. 6.

„Prosím o zvážení možnosti změny ve smlouvě s ohledem na skutečnost, že i chyba kategorie C může být "gramatické nebo pravopisné vady v požadované dokumentaci", což znamená, že za 3 pravopisné chyby v dokumentaci je možné odstoupit od smlouvy. Takový požadavek považujeme za nestandardní. Je možné upravit definici kategorie C?“.

Odpověď zadavatele:

Zadavatel trvá na současném znění. Zadavatel doplňuje, že předmětné ustanovení opravňuje zadavatele odstoupit od smlouvy v daném případě, nikoliv ukládá povinnost od smlouvy odstoupit.

Příloha č. 1 ZD Návrh smlouvy, III. 3.

„Prosíme o zvážení možnosti změny ve smlouvě s ohledem na skutečnosti, že vadou může být i velmi minoritní problém. Je možné smlouvu upravit, tak aby se vztahovalo pouze na vady kritičnosti A?“.

Odpověď zadavatele:

Zadavatel trvá na současném znění.

Příloha č. 1 ZD Návrh smlouvy

„Upozorňujeme, že v návrhu smlouvy není uveden postup a podmínky pro vypořádání při odstoupení od smlouvy. Je možné návrh smlouvy o uvedené doplnit?“.

Odpověď zadavatele:

Odstoupení od smlouvy je upraveno v § 2001 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

Příloha č. 1 ZD Návrh smlouvy

„Upozorňujeme, že v návrhu smlouvy není uvedena definice akceptačních testů, na základě kterých bude prováděna akceptace. Je možné návrh smlouvy o uvedené doplnit?“.

Odpověď zadavatele:

Průběh akceptačního testování je upraven v čl. III návrhu smlouvy – „Testování, předání a převzetí díla“.

Příloha č. 1 ZD Návrh smlouvy

„Upozorňujeme, že v návrhu smlouvy není definována minimální součinnost ze strany Zadavatele. Je možné návrh smlouvy o uvedené doplnit?“.

Odpověď zadavatele:

Z obsahu dotazu dodavatele nevyplývá, v čem konkrétně v souvislosti s návrhem smlouvy spatřuje nedostatečné vymezení součinnosti ze strany zadavatele. Zadavatel k tomuto dodává, že návrh smlouvy předpokládá, že v průběhu realizace zakázky budou mezi sebou komunikovat pověřené osoby smluvních stran doplněné v rámci čl. VIII návrhu smlouvy.

Příloha č. 1 ZD Návrh smlouvy

„Upozorňujeme, že v návrhu smlouvy není definována definice rozsahu samotné dodávky. Je možné návrh smlouvy o uvedené doplnit?“.

Odpověď zadavatele:

Rozsah předmětu plnění je definován v rámci čl. 1 návrhu smlouvy – „Předmět smlouvy“.

Příloha č. 1 ZD Návrh smlouvy

„Je možné v oblasti náhrady škod a sankcí uvést maximální výši náhrady škody? Je možné návrh smlouvy o uvedené doplnit?“.

Odpověď zadavatele:

Zadavatel trvá na současném znění.

Zadavatel s ohledem na odpovědi na výše uvedené dotazy týkající se požadavků zadavatele stanovených v návrhu smlouvy, který je součástí Zadávací dokumentace (příloha č. 1), přistoupil ke změně č. 1 zadávací dokumentace. **Změna č. 1 zadávací dokumentace** bude uveřejněna na profilu zadavatele u předmětné veřejné zakázky na adrese: <https://ezak.cnb.cz>.

S pozdravem

JUDr. Jan Mayer
ředitel odboru obchodního
podepsáno elektronicky

