GFR06594216
ESS

Generální finanční ředitelství
Lazarská 15/7, 117 22 Praha 1

Sekce řízení úřadu
Odbor veřejných zakázek a právních služeb

Č. j.: 65681/16/7500-40175-050417

Vyřizuje: Bc. Nikola Hozáková
Tel.: 296 854 436
E-mail: Nikola.Hozakova@fs.mfcr.cz

2. Dodatečná informace k zadávacím podmínkám dle § 49 odst. 3 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ“)

Veřejná zakázka ve zjednodušeném podlimitním řízení:
„Služby certifikační autority pro Finanční správu České republiky“

Zadavatel: Česká republika – Generální finanční ředitelství, Lazarská 15/7, 117 22 Praha 1

Zadavatel obdržel dne 19. a 23. 5. 2016 žádosti o dodatečné informace k předmětné veřejné zakázce. Zadavatel v souladu s § 49 ZVZ poskytuje dodatečné informace v tomto znění:

Dotaz č. 1 (citace uchazeče):

Jaký je předpokládaný termín uzavření smlouvy?

Odpověď č. 1:
Termín uzavření Smlouvy o poskytování služeb certifikační autority (dále jen „smlouvy“) je závislý na průběhu předmětného zadávacího řízení. Zadavatel uzavře smlouvu s vítězným uchazečem v souladu s § 82 odst. 2 ZVZ. Uzavření smlouvy je předpokládáno v druhé polovině června 2016.

Dotaz č. 2 (citace uchazeče):
Jestliže nebude uzavřena smlouva v předpokládaném termínu, budou posunuty i termíny pro ukončení přípravné fáze, resp. začátek poskytování služeb CA?

Odpověď č. 2:
S posunem zahájení Etapy vydávání certifikátů není počítáno, jelikož vychází ze zákonných povinností Finanční správy České republiky.

Dotaz č. 3 (citace uchazeče):
Jaká bude metodika měření výkonnostních parametrů služby (max. doba vydání certifikátu do 5 sekund, resp. vydání minimálně 2 ks certifikátů za sekundu)?

Odpověď č. 3:
Metodika měření SLA bude určena v Detailním návrhu Služeb CA. Předběžně předpokládáme jako primární nástroj analýzu auditních logů Poskytovatele s možností kontrolního měření ze strany Zadavatele (využití externích testovacích nástrojů - simulované žádosti o certifikát na produkci).

Dotaz č. 4 (citace uchazeče):
Jaké jsou požadavky na webové sídlo – kolik klientů ho může paralelně využívat včetně obsluhy?

Odpověď č. 4:
Zadavatel si není jist přesným významem dotazu. Pokud otázka míří na možnost sdílení platformy Služeb CA s jinými službami Poskytovatele jiným zákazníkům, pak tuto možnost zadavatel připouští, a to v případě, že budou splněny všechny bezpečnostní požadavky a požadovaná SLA. Jestliže otázka míří na očekávaný počet paralelních uživatelských přístupů k Web aplikaci CA, může jej Poskytovatel odvodit z kapacitních a výkonnostních požadavků a očekávaného celkového počtu certifikátů. Cena za Služby CA není závislá na počtu paralelních uživatelských přístupů.

Dotaz č. 5 (citace uchazeče):
Je možné zpřesnit harmonogram přípravy Služeb CA tak, aby byl jasnější jejich začátek a konec, např. uvedením předpokládaného data začátku a konce jednotlivých přípravných bodů?

Odpověď č. 5:
Časování jednotlivých kroků harmonogramu přípravy Služeb CA je v Příloze č. 2 Výzvy k podání nabídky (dále jen „Výzvy“) formulováno jednoznačně ve vztahu ke dvěma hlavním časovým bodům:
1. podpisu smlouvy, který závisí na délce trvání zadávacího řízení, viz odpověď na Dotaz č. 1;
2. zahájení poskytování Služeb CA na produkčním prostředí dle smlouvy, čímž se rozumí termín zahájení Etapy vydávání certifikátů, tj. 1. 9. 2016.

Dotaz č. 6 (citace uchazeče):
V příloze č. 2 Výzvy se v části „Požadavky na Web aplikaci CA“ píše o „HTML rozhraní“. Mají se na všech uváděných prohlížečích/platformách (i mobilních) dát generovat klíče a importovat certifikáty?

Odpověď č. 6:
Ano, podpora generování klíčů, vytvoření žádosti a instalace certifikátu je požadována pro všechny uvedené platformy. Podpora může mít formu klientského kódu, který je součástí Web aplikace CA (např. javascript), samostatné klientské aplikace nebo návodu k manuálnímu postupu uživatele, resp. může jít o kombinaci těchto forem. Nesmí přitom vyžadovat další licence, resp. poplatky nad rámec ceny Služeb CA, od Zadavatele, ani od uživatelů Web aplikace CA. Hlavním cílem je maximalizace uživatelského komfortu uživatele a minimalizace požadavků na technickou podporu (která je rovněž v odpovědnosti Poskytovatele).

Dotaz č. 7 (citace uchazeče):
Do jakého důvěryhodného úložiště má být generován klíčový par a importovat certifikát? Stačí souborová PKCS#12?

Odpověď č. 7:
Toto záleží na možnostech dané platformy - standardní úložiště klíčů, resp. standardní framework pro přístup k úložištím klíčů, se záložní možností exportu do souboru PKCS#12.

Dotaz č. 8 (citace uchazeče):
V příloze č. 2 Výzvy se v části "Integrace DPR a Web aplikace CA" v části "autentizační služba DPR pro Služby CA" píše "Vytvořit náhodný unikátní identifikátor daného požadavek - dále jen authToken". O jaký token se jedná? SAML token nebo Kerberos nebo jiný?

Odpověď č. 8:
Nejedná se o standardizovaný token, ale o sadu autentizačních informací a proces jejich předání formou WebService, způsobem popsaným v Příloze č. 2 Výzvy.

Dotaz č. 9 (citace uchazeče):
Může být telefonická podpora poskytovaná pro pracovníky Zadavatele poskytována i ve slovenském jazyce?

Odpověď č. 9:
V souladu s požadavky Zadavatele na technickou podporu, obsaženými v Příloze č. 2 Výzvy, musí probíhat veškerá komunikace s poplatníky a pracovníky Zadavatele v českém jazyce.

Dotaz č. 10 (citace uchazeče):
Požadavek: Pro potřeby centrálního systému Zadavatele, zejména pro podepisování odpovědí na zprávy poplatníků, je požadován relativně malý počet (desítky) certifikátů.
Dotaz: Jaký bude vyžadován certifikát v centrálních systémech Zadavatele pro podepisování odpovědí? Kvalifikovaný nebo komerční? Jaká je představa registračního procesu a dostupnosti vydání těchto certifikátů?

Odpověď č. 10:
Jde o certifikát vydaný stejnou certifikační autoritou jako certifikáty pro poplatníky. Není požadován certifikát kvalifikovaný. Registrační proces bude upřesněn v Detailním návrhu Služeb CA, ale Zadavatel předpokládá obdobný proces jako u kvalifikovaných nebo komerčních systémových certifikátů. Vydávání těchto certifikátů je předpokládáno formou osobní návštěvy registrační autority v pracovních hodinách po předchozí dohodě.

Dotaz č. 11 (citace uchazeče):
Požadavek: Kryptografické parametry a platnost certifikátů

Certifikát CA	Maximální doba platnosti	6 let
Certifikát CA	Aktivní období certifikátu	3 roky

Dotaz: Skutečně má být omezena platnost certifikátu podřízené CA na 6 let? Předpokládáme, že jako kořenový certifikát CA bychom využili náš stávající s platností 15 let (končí v roce 2025) a pouze bychom vytvořili novou podřízenou CA, která by vydávala certifikáty pro EET.

Odpověď č. 11:
Delší období platnosti certifikátů CA je přípustné za následujících podmínek:
1) Aktivní období certifikátu musí skončit minimálně 3 roky před platností certifikátu.
2) Po třech letech dojde ke společné revizi aktuálnosti použitých kryptografických algoritmů vzhledem k technologickému vývoji v oblasti kryptografie a podle výsledku bude naplánováno dřívější ukončení aktivního období certifikátu CA nebo termín další revize (nejpozději opět za 3 roky).

Dotaz č. 12 (citace uchazeče):
Požadavek: Frekvence vydávání CRL musí být určena Poskytovatelem v detailním návrhu a schválena Zadavatelem, maximální možné požadavky jsou:
• pravidelný interval vydávání CRL 15 minut
• vydání nového CRL do 1 minuty od zneplatnění certifikátu

Dotaz: Jaká je požadovaná platnost CRL? Standardně bývá platnost 24 hodin.

Odpověď č. 12:
Všechny uvedené parametry CRL budou upřesněny v Detailním návrhu Služeb CA. Maximální (nejtvrdší) požadavky uvedené ve smlouvě jsou formulovány z pohledu

klientských zařízení, které pravidelně aktivně kontrolují aktuálně platné CRL. Z tohoto pohledu není platnost CRL zásadním kritériem. Předběžně lze tedy prohlásit, že 24 hodin je přijatelnou hodnotou.

Dotaz č. 13 (citace uchazeče):

Požadavek: Služby Web aplikace CA

Web aplikace CA musí podporovat následující funkce pro poplatníky uživatelsky přívětivou formou (detailní návrh funkcionality musí být rozpracován Poskytovatelem v detailním návrhu a schválen Zadavatelem):

• Podpora generování klíčů na straně poplatníka, vytvoření žádosti o certifikát (CSR - Certificate Signing Request) a instalaci certifikátu. Web aplikace CA zpřístupní poplatníkovi potřebné klientské nástroje a návody.

Web aplikace CA musí podporovat následující klientské platformy ve verzích podporovaných jejich výrobci v k 1. 1. 2016 a novějších:

- web prohlížeče Chrome, Firefox, Internet Explorer, Safari
- operační systémy a odpovídající standardní web prohlížeče mobilních zařízení: iOS, Android, Windows Phone a Windows 10

Dotaz: Webová aplikace nemůže generovat žádosti o certifikát z důvodu neexistujících nástrojů pro všechny požadované platformy. Navrhujeme, aby generování žádostí probíhalo pomocí externích klientských aplikací. Webová aplikace by pouze zpracovávala vytvořený CSR ve standardu PKCS#10, popř. ID CSR uloženého v systému PostSignum. Můžeme to takto nabídnout? Používáme aplikace iSignum (OS Windows) a Signer (iOS, Android, Windows Phone).

Odpověď č. 13:

Podpora generování klíčů, vytvoření žádosti a instalace certifikátu je požadována pro všechny uvedené platformy. Podpora může mít formu klientského kódu, který je součástí Web apikace CA (např. javascript), samostatné klientské aplikace nebo návodu k manuálnímu postupu uživatele, resp. může jít o kombinaci těchto forem. Nesmí přitom vyžadovat další licence, resp. poplatky nad rámec ceny Služeb CA, od Zadavatele ani od uživatelů Web aplikace CA. Hlavním cílem je maximalizace uživatelského komfortu uživatele a minimalizace požadavků na technickou podporu (která je rovněž v odpovědnosti Poskytovatele).

Dotaz č. 14 (citace uchazeče):

Požadavek: Web aplikace CA musí podporovat synchronní i asynchronní mód vydání certifikátu, přičemž

• Pokud je možné vydat certifikát do požadovaného času vydání (5 sec), odpověď (certifikát) na CSR musí být uživateli vrácena synchronně v rámci jednoho HTTPS dotazu.

Dotaz: Synchronní mód považujeme za velice problematické řešení při velkém množství žádostí. Toto řešení by vyžadovalo velký počet udržovaných spojení se serverem. To by mohlo vést k nestabilitě systému. Navrhujeme používat pouze asynchronní mód. Je synchronní mód striktně vyžadován?

Odpověď č. 14:

V rámci formulovaných SLA, resp. kapacitních a výkonnostních požadavků, odpovídá požadavek vydání certifikátu do 5 sec zátěži nižší než 2 certifikáty za sec. To odpovídá požadavku na minimálně 10 paralelních „dlouhotrvajících“ spojení se serverem, což nepovažujeme za neúměrnou zátěž.

Dotaz č. 15 (citace uchazeče):

Požadavek: Pokud to není možné, přejde Web aplikace CA do asynchronního módu – uživatel dostane jako odpověď potvrzení o přijetí žádosti a indikaci času vydání certifikátu.

Při další návštěvě Web aplikace CA mu musí být nabídnut seznam nových asynchronně vydaných certifikátů.
Poznámka: Vzhledem k tomu, že množství vydávaných certifikátů může probíhat v nepravidelných špičkách, nelze přesně predikovat čas vydání certifikátu. Tento čas může být pouze orientační.

Odpověď č. 15:
Ano, termínem „indikace času“ je míněn orientační časový údaj.

Dotaz č. 16 (citace uchazeče):
Požadavek: Web aplikace CA musí podporovat konfigurovatelný mechanismus řízení tempa vydávání certifikátů jednoho poplatníka. Mechanismus řízení tempa vydávání certifikátů bude vycházet z parametru maximálního očekávaného počtu certifikátů poplatníka, kalkulovaného na základě počtu provozoven (který obdrží přes integrační rozhraní od DPR) a konfigurovatelných globálních parametrů. Parametr maximálního očekávaného počtu certifikátů poplatníka musí být možné pro jednotlivé poplatníky manuálně změnit prostřednictvím požadavku na technickou podporu poplatníků. Mechanismus řízení tempa vydávání certifikátů bude aktivován při zpracování CSR poplatníka, který má více platných certifikátů vydaných v průběhu jednoho roku zpětně než maximální očekávaný počet certifikátů poplatníka - Web aplikace CA přejde do asynchronního módu a bude zpracovávat CSR tohoto poplatníka a vydávat certifikáty zpomaleným tempem (např. 1 certifikát denně - konfigurovatelný parametr).
Dotaz: Co je smyslem této funkce? Při analýze této funkcionality vzniká obrovská pracnost. Je tato funkcionalita striktně vyžadovaná?

Odpověď č. 16:
Ano. Smyslem této funkce je primárně omezení „útoků“ na Služby CA formou čerpání velkého množství nepotřebných certifikátů a obecně zajištění efektivního využívání Služeb CA ze strany poplatníků.

Dotaz č. 17 (citace uchazeče):
Požadavek: Vzhledem k rozsahu požadovaných činností (které převyšují prezentované požadavky na osobní schůzce – především požadavky na webovou aplikaci CA) je velice krátká fáze Příprava služeb CA.
Dotaz: Je možné tuto fázi rozdělit na více částí dle priorit s tím, že by části s nižší prioritou byly dokončeny až ve fázi vydávání certifikátů? Samozřejmě s tím, že by čas zahájení fáze vydávání certifikátů zůstal nezměněn.

Odpověď č. 17:
V rámci Detailního návrhu Služeb CA je možné (po odsouhlasení Zadavatelem) rozdělit fázi testování na menší úseky a určit kritické a nekritické prvky funkcionality pro jednotlivé úseky testování. Časově nejkritičtějšími prvky funkcionality jsou integrace DPR a Web aplikace CA, vydávání certifikátů a související funkcionality Web aplikace CA. Implementace všech funkcí a všechny fáze testování ale musí skončit před zahájením Etapy vydávání certifikátů.

Dotaz č. 18 (citace uchazeče):
Požadavek: Součástí akceptace přípravy Služeb CA bude penetrační bezpečnostní test, provedený organizací pověřenou Zadavatelem. Penetrační test bude proveden minimálně v rozsahu dle OWASP 4.
V rámci bezpečnostních testů bude dále provedena kontrola souladu technického řešení a režimu provozu technické provozní platformy Služeb CA s uvedenými bezpečnostními požadavky, normami a standardy. Kontrolován bude soulad dokumentace s uvedenými normami a soulad reality s dokumentací.

Dotaz: Náklady za provedení bezpečnostního testu pověřené organizaci hradí Zadavatel nebo musí být součástí kalkulace nabídky?

Odpověď č. 18:
Náklady za provedení bezpečnostního testu pověřené organizaci hradí Zadavatel. Poskytovatel je odpovědný pouze za opravu chyb nalezených v testech a nezbytnou součinnost s provedením testů.

Zadavatel neprodlužuje lhůtu pro podání nabídek.

V souladu s ustanovením § 49 odst. 3 ZVZ zadavatel odesílá tyto dodatečné informace všem uchazečům, kteří požádali o Výzvu vč. zadávací dokumentace nebo kterým byla Výzva vč. zadávací dokumentace poskytnuta a dále bude dodatečná informace vyvěšena na profilu zadavatele https://mfcr.ezak.cz/profile_display_49.html.

Mgr. Anna Bednářová
ředitelka odboru

Elektronicky podepsáno
23.05.2016
Mgr. Anna Bednářová
ředitelka odboru